Aug. 16, 2013

SP 800-161

DRAFT Supply Chain Risk Management Practices for Federal Information Systems and Organizations

This document provides guidance to federal departments and agencies on identifying, assessing, and mitigating Information and Communications Technology (ICT) supply chain risks at all levels in their organizations. It integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance.

Due to the recent government shutdown, NIST is extending the comment period for NIST SP 800-161 by 14 days. Comments are now due by ***November 1, 2013***. Please submit comments to scrm-nist@nist.gov with "Comments NIST SP 800-161" in the subject line. A template for submitting comments is provided below.

NIST Special Publication 800-161

Initial Public Draft

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

Rama Moorthy
Hatha Systems

Nadya Bartol
Utilities Telecom Council

Stephanie A. Shankles
Booz Allen Hamilton

August 2013

U.S. Department of Commerce
Penny Pritzker, Secretary

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

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

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

National Institute of Standards and Technology Special Publication 800-161
Natl. Inst. Stand. Technol. Spec. Publ. 800-161, 285 pages (August 2013)
http://dx.doi.org/10.6028/NIST.SP.161
CODEN: NSPUE2

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 NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

Public comment period: August 16, 2013 through October 15, 2013

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

Reports on Computer Systems Technology

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

Abstract

The information and communications technology (ICT) supply chain is a complex, globally distributed system of interconnected networks that are logically long, with geographically diverse routes and multiple tiers of outsourcing. This system of networks includes organizations, people, processes, products, and services and the infrastructure supporting the system development life cycle, including research and development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement) of an organization's ICT products (i.e., hardware and software) and services.

Today's ICT supply chains have increased complexity, diversity, and scale, while federal government information systems have been rapidly expanding in terms of capability and number, with an increased reliance on outsourcing and commercially available products. These trends have caused federal departments and agencies to have a lack of *visibility* and *understanding* throughout the supply chain of how the technology being acquired is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. This lack of visibility and understanding, in turn, has decreased the *control* federal departments and agencies have with regard to the decisions impacting the inherited risks traversing the supply chain and the ability to effectively manage those risks.

NIST Special Publication (SP) 800-161 provides guidance to federal departments and agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels in their organizations. NIST SP 800-161 integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance.

Keywords

Acquirer, Criticality Analysis, External Service Provider, Information and Communication Technology (ICT), Integrator, Risk Management, Supplier, Supply Chain,

Acknowledgements

The authors, Jon Boyens, National Institute of Standards and Technology (NIST), Celia Paulsen (NIST), Rama Moorthy (Hatha Systems), Nadya Bartol (Telecommunications Utilities Council) and Stephanie Shankles (Booz Allen Hamilton), would like to acknowledge and thank the information and communication technology (ICT) supply chain risk management (SCRM) community, which has provided the authors invaluable insight and diverse perspectives to managing the ICT supply chain. We would especially like to thank the participants of NIST's October 2012 ICT SCRM Workshop for providing the guiding foundation to the approach this publication has taken.

Notes to Reviewers

NIST Special Publication 800-161 represents the evolution of a five-year public/private initiative to develop guidance for ICT SCRM. The document is written for use by the federal departments and agencies that acquire ICT products and services. The document is consistent with the Joint Task Force Transformation Initiative Unified Information Security Framework and integrates concepts described in a number of NIST publications to facilitate integration with the agencies' operational activities.

Your feedback to us during the public review period is invaluable as we attempt to provide useful and practical ICT SCRM guidance to federal agency acquirers. Specifically, we would very much welcome your feedback on the following:

- Relationship of ICT SCRM to the overall risk management process;
- Completeness of ICT SCRM guidance for Tiers 1, 2, and 3;
- Usability of the ICT supply chain risk assessment process;
- Clarity of criticality analysis process;
- Usability and readability of how ICT SCRM controls are presented;
- Relationship of ICT SCRM controls to NIST SP 800-53 Rev4 controls;
- New supply chain controls and control enhancements; and
- Threat scenarios.

Regarding the threat scenarios, NIST has been receiving feedback from both the public and private sectors for the last five years about the need to provide threat scenarios that demonstrate ICT SCRM concerns and risk-based ways to address those. The threat scenarios are a response to that feedback. Your feedback is requested as to whether the example framework and the example scenarios are practical and realistic. Suggestions of edits or alternative frameworks with practical and realistic examples are very welcome.

TABLE OF CONTENTS

CHAPTER ONE INTRODUCTION 1

1.1 PURPOSE AND APPLICABILITY 4

1.2 TARGET AUDIENCE.. 6

1.3 RELATIONSHIP TO OTHER PUBLICATIONS 6

1.4 FOUNDATIONAL PRACTICES.. 7

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION 9

CHAPTER TWO INTEGRATION OF ICT SCRM INTO ORGANIZATION-WIDE RISK MANAGEMENT 10

2.1 MULTITIERED RISK MANAGEMENT.. 11

2.1.1 TIER 1 – ORGANIZATION 13

2.1.2 TIER 2 – MISSION/BUSINESS PROCESS................................ 14

2.1.3 TIER 3 – INFORMATION SYSTEMS 14

2.2 ICT SCRM ACTIVITIES IN RISK MANAGEMENT PROCESS .. 15

2.2.1 FRAME.. 17

2.2.2 ASSESS 26

2.2.3 RESPOND 34

2.2.4 MONITOR... 39

CHAPTER THREE ICT SCRM CONTROLS 43

3.1 ICT SCRM CONTROLS OVERLAY.. 43

3.2 ICT SCRM CONTROLS THROUGHOUT ORGANIZATIONAL HIERARCHY.. 44

3.3 APPLYING ICT SCRM CONTROLS TO ACQUIRING ICT PRODUCTS AND SERVICES 44

3.3.1 SYSTEM INTEGRATORS... 45

3.3.2 SUPPLIERS.. 45

3.3.2 EXTERNAL PROVIDERS OF INFORMATION SYSTEM SERVICES.. 46

3.4 SELECTING, TAILORING, AND IMPLEMENTING ICT SCRM SECURITY CONTROLS 46

3.4.1 EXAMPLE ICT SCRM CONTROL FORMAT 47

3.4.2 USING ICT SCRM CONTROLS IN THIS DOCUMENT 48
3.5 ICT SCRM SECURITY CONTROLS.. 49
APPENDIX A GLOSSARY.. 108
APPENDIX B ACRONYMS 116
APPENDIX C REFERENCES.. 119
APPENDIX D NIST SP 800-53 ICT SCRM-RELEVANT CONTROLS... 122
APPENDIX E ICT SUPPLY CHAIN THREAT EVENTS................ 254
APPENDIX F SUPPLY CHAIN THREAT SCENARIOS AND FRAMEWORK.. 261

TABLE OF TABLES AND FIGURES

Figure 1-1. ICT Supply Chain Risk 3
Figure 1-2. Four Aspects of ICT SCRM.. 4
Figure 2-1. Risk Management Process 10
Figure 2-2: Mulitiered Organization-wide Risk management 12
Table 2-1: Supply Chain Risk Management Stakeholders 12
Figure 2-3. ICT SCRM Activities in Risk Management Process 16
Figure 2-4. ICT SCRM Risk Assessment.. 17
Figure 2-5. ICT SCRM in the Frame Step... 18
Table 2-4. Example ICT Supply Chain Threat Agents.. 20
Table 2-5. Supply Chain Threat Considerations... 21
Table 2-6. Supply Chain Vulnerabilities Considerations 22
Table 2-7. Supply Chain Constraints.. 24
Figure 2-6. ICT SCRM in the Assess Step 27
Table 2-8: Examples of ICT Supply Chain Vulnerabilities Mapped to the Organizational Tiers 31
Figure 2-7. ICT SCRM in the Respond Step 35
Table 2-9. ICT SCRM Plan Controls at Tiers 1, 2, and 3... 38
Figure 2-8. ICT SCRM in the Assess Step 40
Table 3-1. ICT SCRM Control Families.. 44
Table 3-2. Example ICT SCRM Control Format... 47

Table E-1. Adversarial ICT Supply Chain Threat Events 254
Table E-1. Adversarial ICT Supply Chain Threat Events 259

CHAPTER ONE

INTRODUCTION

THE information and communications technology (ICT) supply chain is a complex, globally distributed system of interconnected networks that are logically long, with geographically diverse routes and multiple tiers of outsourcing. This system of networks includes organizations, people, processes, products, and services and the infrastructure supporting the system development life cycle, including research and development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement) of an organization's ICT products (i.e., hardware and software) and services. Today's ICT supply chains have increased complexity, diversity, and scale, while federal government information systems have been rapidly expanding in terms of capability and number, with an increased reliance on outsourcing and commercially available products. These changes have resulted in a reduction in ***visibility*** and ***understanding*** of federal departments and agencies throughout the supply chain, including how the technology being acquired is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. This lack of visibility and understanding, in turn, has decreased the ***control*** federal departments and agencies have with regard to the decisions impacting the inherited risks traversing the supply chain and the ability to effectively mitigate those risks.[1, 2]

In ICT supply chain, system integrators have a distinct role of assembling information systems, information system components, and information services developed by developers. These components and systems may be developed by other parties also known as vendors or product resellers. NIST SP 800-161 splits the NIST SP 800-53 Rev4 *developer* into *system integrator* and

[1] This document adapts the definition of risk from Federal Information Processing Standard (FIPS) 200 to establish a definition for ICT supply chain risk as follows:

> *Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.*

[2] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53 Rev4), defines developer as:

> *A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.*

supplier. In this context, *system integrator* refers to item (ii) in the NIST SP 800-53 Rev4 definition, while *Supplier* refers to items (i), (iii), and (iv). [3]

The risks resulting from relevant ICT supply chain threats exploiting existing vulnerabilities are either reduced functionality or unwanted functionality present on the systems that support an organization's mission. Specifically, reduced functionality[4] may result from poor quality ICT that is assumed to be of good quality or from counterfeit components. Unwanted functionality[5] may result from insertion of malicious software or from poor quality software and may enable theft of intellectual property (IP). Compromised ICT products and services may lead to both reduced and unwanted functionality. ICT supply chain risks include insertion of counterfeits, tampering, theft, and insertion of malicious software.

While non-adversarial and quite unintentional, poor manufacturing and development practices may also result in ICT supply chain risks such as weak or vulnerable code, spillage of sensitive or proprietary information, or loss of equipment. ICT products and services are vulnerable to various intentional and unintentional (or adversarial/non-adversarial) threats as they traverse the supply chain. In general, while vulnerabilities may exist due to a variety of reasons, they are not always identified or resolved. Once hardware or software that contains these vulnerabilities is installed into an operational system, the vulnerabilities can be exploited later, at an unknown point in time. In other words, it may take years for the vulnerability stemming from the ICT supply chain to be exploited or discovered. The resulting reduced or unwanted functionality may have a negative impact of federal agencies' missions that could range from reduction in service levels resulting in customer dissatisfaction to theft of intellectual property, or degradation of mission-critical federal agency functions.

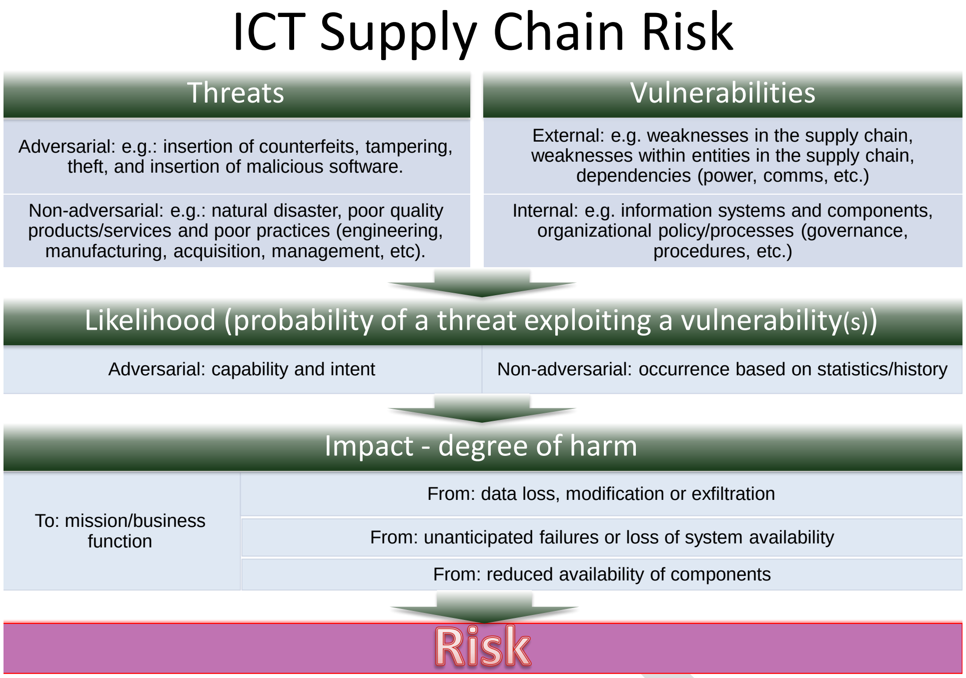
Figure 1-1 depicts ICT supply chain risk resulting from the likelihood and impact of the applicable threats exploiting applicable vulnerabilities.

[3] This document defines compromise as:

> *An ICT Supply Chain Compromise is an occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service.*

[4] Reduced functionality occurs when acquired ICT does not meet expected or required standards and may **result from poor quality or counterfeit products.**

[5] Unwanted functionality occurs when acquired products or services have additional or unexpected properties which may pose a threat to the organization and may result from the insertion of malicious software or poor quality.



ICT Supply Chain Risk

Threats

Adversarial: e.g.: insertion of counterfeits, tampering, theft, and insertion of malicious software.

Non-adversarial: e.g.: natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc).

Vulnerabilities

External: e.g. weaknesses in the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, etc.)

Internal: e.g. information systems and components, organizational policy/processes (governance, procedures, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent

Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function

From: data loss, modification or exfiltration

From: unanticipated failures or loss of system availability

From: reduced availability of components

Risk

Figure 1-1. ICT Supply Chain Risk

Globalization of the commercial ICT marketplace provides increased opportunities for adversaries (individuals, organizations, or nation-states) to directly or indirectly affect the management or operations of companies in a manner that may result in risks to the end user. For example, a foreign nation-state may have the power to coerce a manufacturer to hand over the manufacturing specifications of a sensitive U.S. system or to insert malicious capability into a product. Threats and vulnerabilities created in this way are often extremely sophisticated and difficult to detect and thus provide a significant risk to agencies. However, ICT products or services manufactured anywhere (domestically or abroad) may contain vulnerabilities that can present opportunities for ICT supply chain-related compromises, including most of the same sophisticated threats that are posed by foreign entities.

ICT SCRM lies at the intersection of integrity, security, resiliency, and quality, as depicted in Figure 1-2. Security is important for protecting information that describes the ICT supply chain (e.g., information about the paths of ICT products and services, both logical and physical), traverses the ICT supply chain (e.g., intellectual property contained in ICT products and services), and information about the parties participating in the ICT supply chain (anyone who touches an ICT product or service throughout its life cycle). Integrity is important for ensuring that the ICT products or services in the ICT supply chain are genuine and authentic and do not contain any unwanted (and potentially dangerous) functionality, as well as that the ICT products and services will perform according to expectations. Resiliency is important for ensuring that ICT supply chain will provide required ICT products and services under stress. Quality is important to reduce unintentional vulnerabilities that provide opportunities for exploitation.

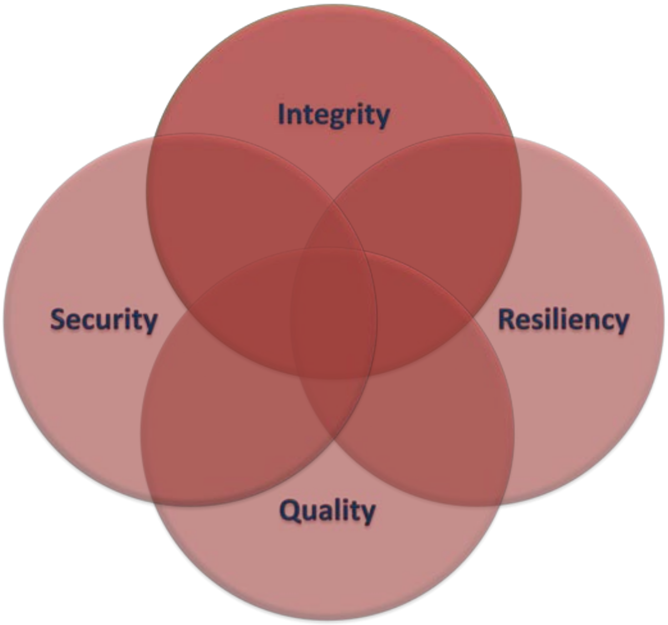


Figure 1-2. Four Aspects of ICT SCRM

Currently, federal departments and agencies and many private sector integrators and suppliers use varied and nonstandard practices, which make it difficult to consistently manage and measure ICT supply chain risks across different organizations. Meanwhile, due to the growing sophistication and complexity of ICT and the global ICT supply chains, federal agency information systems are increasingly at risk of compromise, and agencies need guidance to help manage ICT supply chain risks.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidance to federal agencies on selecting and implementing mitigating processes and controls at all levels in their organizations to help manage risks to or through ICT supply chains.

This document is consistent with the Joint Task Force Transformation Initiative Unified Information Security Framework[6] and uses concepts described in a number of NIST publications

[6] **Unified Information Security Framework** is a comprehensive, flexible, risk-based information security framework developed by the Joint Task Force, a partnership among the National Institute of Standards and Technology, the Department of Defense, the U.S. Intelligence Community, and the Committee on National Security Systems. The Unified Information Security Framework consists of five core publications including: **NIST Special Publication 800-39** (Managing Information Security Risk: Organization, Mission, and Information System View); **NIST Special Publication 800-30** (Guide for Conducting Risk Assessments); **NIST Special Publication 800-53** (Security and

to facilitate integration with the agencies' operational activities. These publications are complementary in nature and work together to help organizations build risk-based information security programs to help protect organizational operations and assets against a range of diverse and increasingly sophisticated threats. This document empowers organizations to develop specialized ICT SCRM solutions that are tailored to their particular mission/business needs, operational environments, and/or implementing technologies. This document will be revised to remain consistent with the NIST SP800-53 security controls catalog, using an iterative process as the ICT SCRM discipline matures.

NIST SP 800-161 applies the multi-tiered risk management approach of NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, by providing guidance at Organization, Mission, and Systems Tiers. The processes in this document are integrated into the Risk Management Process described in NIST SP 800-39 to facilitate integration of ICT SCRM into the overall federal agency risk management activities. This guidance contains an enhanced overlay of specific ICT SCRM controls, based on NIST SP 800-53 Rev4.It refines and expands NIST SP 800-53 Rev4 controls, adds new controls that specifically address ICT SCRM, and offers SCRM-specific supplemental guidance where appropriate. These processes and controls should be integrated into agencies' existing system development life cycles (SDLC) and organizational environments at all levels of the risk management hierarchy (organization, mission, system). For individual systems, this guidance is recommended for use for those information systems that are categorized as high-impact systems according to the Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. The agencies may choose to apply this guidance to system components or to specific systems at a lower impact level. Finally, NIST SP 800-161 describes the planning and implementation of an ICT SCRM plan to be developed at all levels of an organization. An ICT SCRM plan is an output of ICT supply chain risk assessment and should contain ICT SCRM controls tailored to specific agency mission/business needs, operational environments, and/or implementing technologies.

The guidance/controls contained in this document are built on existing practices from multiple disciplines 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 systems, products, and services. It should be noted that this document gives federal agency acquirers (also referenced as 'organization' throughout the document) the flexibility to either develop stand-alone documentation (e.g. policies, assessment and authorization (A&A) plan and source selection plan (SSP)) for ICT SCRM or to integrate it into existing agency documentation.

Privacy Controls for Federal Information Systems and Organizations); **NIST Special Publication 800-53A** (Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans); and **NIST Special Publication 800-37** (Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach).

As a result of implementing the guidance in this document, organization will be able to set up appropriate policies, processes, and controls to manage ICT supply chain risks to their mission.

1.2 TARGET AUDIENCE

The audience for this document is federal agency personnel involved in engineering/developing, testing, deploying, acquiring, maintaining, and retiring a variety of ICT components and systems. However, other organizations are free to make use of the guidance in as much as it applies to their situation. ICT supply chain is an enterprise-level activity that should be directed under the overall agency governance, regardless of the specific organizational structure. Specifically, ICT supply chain risk management activities should be led by the risk executive function, described in NIST SP 800-39. Implementing ICT SCRM requires federal departments and agencies to establish a coordinated team-based approach to assess the ICT supply chain risk and manage this risk by using technical and programmatic mitigation techniques. The coordinated team approach, either ad hoc or formal, will enable agencies to conduct a comprehensive analysis of their ICT supply chain, communicate with external partners/stakeholders, and provide appropriate resources to the individual responsible for a specific acquisition in developing an ICT supply chain strategy for that acquisition.

Members of the ICT SCRM team should be a diverse group of people who are involved in the various aspects of the SDLC. Collectively, to aid in supply chain risk management, these individuals should have an awareness and provide expertise in organizational acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.

The ICT SCRM team consists of members with diverse roles and responsibilities for leading and supporting ICT SCRM activities including information technology, information security, contracting, risk executive function, mission/business, legal, supply chain and logistics, acquisition and procurement, and other related functions. They are the intended users of this document. These individuals may include government personnel or prime contractors hired to provide acquisition services to a government client.

1.3 RELATIONSHIP TO OTHER PUBLICATIONS

NIST SP 800-161 extends the fundamental concepts described in:

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, to integrate ICT SCRM into the risk management tiers and risk management process;
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessment s* (NIST SP 800-30Rev1), to integrate ICT SCRM into the risk assessment process;
- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, to conduct criticality analysis to scoping ICT SCRM activities high impact components or systems;

- NIST 800-53 Rev4, *Security and Privacy Controls for Federal Information Systems and Organizations*, to provide information security controls for expansion and tailoring to ICT SCRM context; and
- NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, *Building Effective Security Assessment Plans*

NIST SP 800-161 draws from a collaborative ICT SCRM community workshop hosted in October 2012 and NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems,* [7] which resulted from several years of rigorous study of the ICT SCRM discipline and provided NIST the insight required to scope and develop this special publication. NISTIR 7622 can be used by the reader for background materials in support of applying the special publication to their specific acquisition processes.

NIST SP 800-161 also draws from several external publications, including:

- National Defense University, Software Assurance in Acquisition: Mitigating Risks to the Enterprise;
- National Defense Industrial Association (NDIA), Engineering for System Assurance;
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288 – System Lifecycle Processes;
- Draft ISO/IEC 27036 – Information Technology – Security Techniques – Information Security for Supplier Relationships; and
- Open Trusted Technology Provider Standard (O-TTPS)™, Version 1.0, Mitigating Maliciously Tainted and Counterfeit Products
- Software Assurance Forum for Excellence in Code (SAFECode) Software Integrity Framework and Software Integrity Best Practices.

1.4 FOUNDATIONAL PRACTICES

ICT supply chain risk management requires collaboration among different disciplines. Furthermore, it builds upon the foundation provided by these multiple disciplines and is enabled by mature standardized implementation of basic organizational practices. Such basic organizational practices include ensuring that federal department and agency acquirers understand the cost and scheduling constraints of implementing ICT SCRM, integrating information security requirements into the acquisition process, using applicable baseline security controls as one of the sources for security requirements, ensuring a robust software quality control process, and establishing multiple delivery routes for critical system elements.

Federal departments and agencies should take an incremental approach and ensure that they first reach a base level of maturity in these organizational practices prior to specifically focusing on

[7] NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems,* October 2012. http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

ICT SCRM that are more advanced. The base level of maturity can include a formal program and or process implementation with dedicated resources (part and full time). To do so, federal departments and agencies should carefully consider validating that the foundational practices are mature and comparable to those of the integrators and suppliers so that maximum value is gained from applying the ICT SCRM processes and the specific controls and guidance in this document. Those foundational practices are described in NIST standards and guidelines and other applicable national and international standards and best practices. Having foundational practices in place is critical to successfully and productively interacting with mature integrators and suppliers who may have such practices standardized and in place. It is expected that FIPS 199 high-impact systems already have these foundational practices established.

The following are specific examples of the foundational practices that can improve an organization's ability to develop and implement specific ICT SCRM practices:

- Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39) including an organization-wide risk assessment process (in accordance with NIST SP 800-30);
- Establish an organization governance structure that integrates ICT SCRM requirements and incorporates these requirements into the organizational policies;
- Establish consistent, well-documented, repeatable processes for determining FIPS 199 impact levels;
- Use risk assessment processes after the FIPS 199 impact level has been defined, including criticality analysis, threat analysis, and vulnerability analysis;
- Implement Quality and reliability program that includes quality assurance and quality control process and practices;
- Establish a set of roles and responsibilities for ICT SCRM that ensures that the broad set of right individuals are involved in decision making, 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 (e.g., Legal, Risk Executive, HR, Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/procurement, supply chain logistics, etc.);
- Ensure adequate resources are allocated to information security and ICT SCRM to ensure proper implementation of guidance and controls;
- Implement consistent, well-documented, repeatable processes for system engineering, ICT security practices, and acquisition;
- Implement an appropriate and tailored set of baseline information security controls in NIST SP 800-53 Revision 4;
- Implement a tested and repeatable contingency plan that integrates ICT supply chain risk considerations to ensure the integrity and reliability of the supply chain including during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor strikes); and
- Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying causes of security incidents, including those originating from the ICT supply chain.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

This document is organized as follows:

- Chapter 1 provides purpose, scope, and applicability of the document and describes foundational concepts and practices.
- Chapter 2 discusses ICT SCRM processes and how to integrate them into the organizational risk management hierarchy and risk management process, based on NIST SP 800-39.
- Chapter 3 provides a comprehensive set of baseline controls for organizations to choose from and the guidance required for customization/tailoring for their organization and ICT needs.
- Appendix A provides a glossary of terms used in this document.
- Appendix B provides acronyms and abbreviations used in this document.
- Appendix C lists references used in the development of this document.
- Appendix D provides NIST SP 800-53 Rev4 controls relevant to ICT SCRM that are listed or expanded in Chapter 3.
- Appendix E provides a listing of threats for NIST SP 800-30 Rev1 Appendix E relevant to ICT SCRM.
- Appendix F provides Supply Chain Threat Scenarios and Analysis Framework.

CHAPTER TWO

INTEGRATION OF ICT SCRM INTO ORGANIZATION-WIDE RISK MANAGEMENT

ICT Supply Chain risk management should be integrated into organization-wide risk management process described in NIST SP 800-39, and depicted in Figure 2-1, that includes the following steps:

(i) Frame risk – establish the context for risk-based decisions and the current state of the system or ICT supply chain environment;

(ii) Assess risk – review and interpret threat, vulnerability, and related information;

(iii) Respond to risk once determined – select, tailor, and implement mitigation controls; and,

(iv) Monitor risk on an ongoing basis, including changes to an information system or ICT supply chain environment, using effective organizational communications and a feedback loop for continuous improvement.

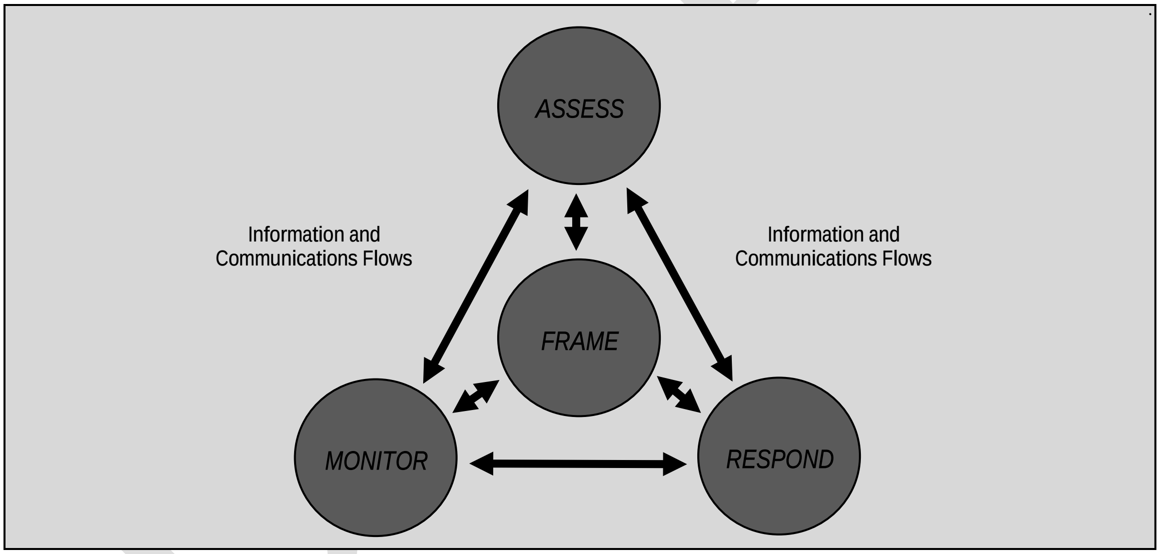

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Figure 2-1. Risk Management Process

Managing ICT supply chain risks is a complex, multifaceted undertaking that requires a coordinated effort across an organization,[8] including engaging multiple disciplines in identifying priorities and developing solutions, ensuring that ICT SCRM activities are performed throughout the SDLC, and incorporating ICT SCRM into overall risk management decisions. ICT SCRM

[8] "Organization" is defined as an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). (FIPS 200, adapted)

activities should involve identifying and assessing applicable risks, determining appropriate mitigating actions, developing an ICT SCRM Plan to document selected mitigating actions, and monitoring performance against the ICT SCRM Plan. Because ICT supply chains differ across and within organizations, the ICT SCRM plan should be tailored to individual organizational contexts. A tailored ICT SCRM plan will help organizations focus appropriate resources on the most critical functions and components based on organizational mission/business requirements and their risk environment.

This chapter describes how ICT SCRM depends on each tier of an organization. This spans senior leaders providing the strategic direction, mid-level leaders planning and managing projects, and individuals on the front lines developing, implementing, and operating the systems supporting the supply chain. The activities performed in each tier can be integrated into an organization's overall risk management process in order to ensure that the ICT SCRM program appropriately supports the organization's mission and goals.[9]

Section 2.1 describes the three-tier risk management approach in terms of ICT SCRM. Section 2.2 describes the Risk Management Framework as it applies to ICT SCRM. Both concepts are described in greater detail in NIST SP 800-39.

2.1 MULTI-TIERED RISK MANAGEMENT

To integrate risk management throughout the organization, NIST 800-39 describes a three-tier approach, depicted in Figure 2-2, that addresses risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. ICT SCRM requires the involvement of all three tiers.

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

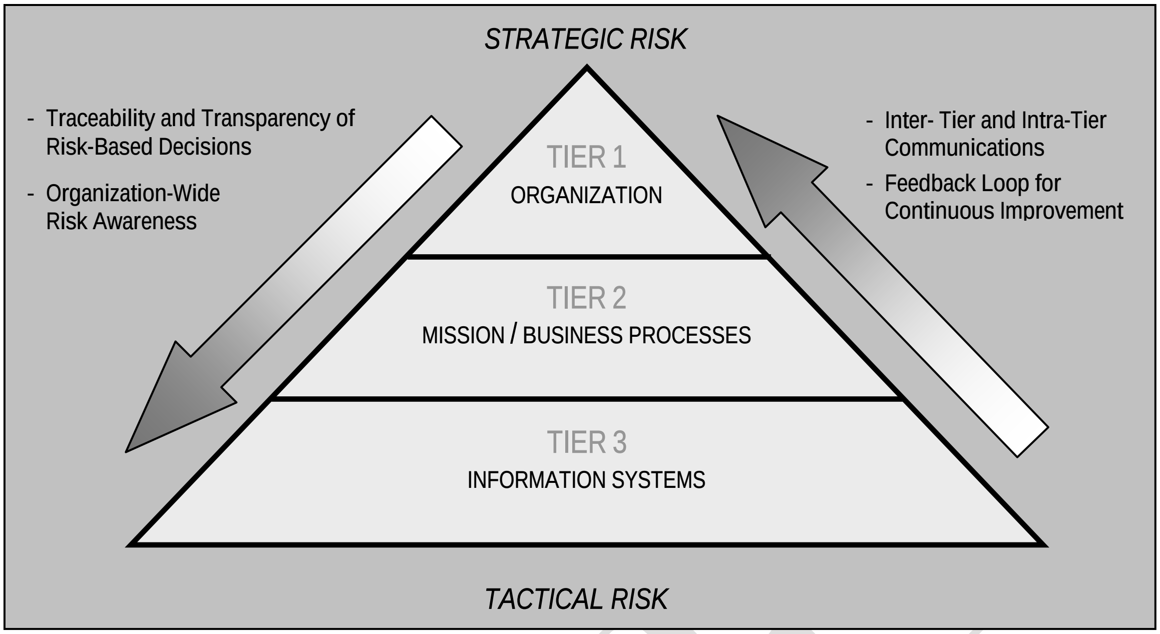

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TACTICAL RISK

Figure 2-2: Multitiered Organization-wide Risk Management

Tier 1 is engaged in the development of the overall ICT SCRM strategy, determination of enterprise-level ICT SCRM risks, and setting of the enterprise-level ICT SCRM policies to guide the federal agency activities in establishing and maintaining enterprise-wide ICT SCRM capability. Tier 2 is engaged in prioritizing the federal agency mission and business functions, conducting mission/business-level risk assessment, implementing Tier 1 strategy and guidance to establish the overall federal agency organizational capability to manage ICT supply chain risks, and guiding agency-wide IT acquisitions and their corresponding SDLCs. Tier 3 is involved in specific ICT SCRM activities to be applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' SDLCs. The ICT SCRM activities can be performed by a variety of individuals or groups within a federal agency ranging from a single individual to committees, divisions, or any other organizational structures. ICT SCRM activities will be different for different organizations depending on their organizations structure, culture, mission, and many other factors.

Table 2-1 shows generic ICT SCRM stakeholders for each tier with the specific ICT SCRM activities performed within the corresponding tier. These activities are either direct ICT SCRM activities or have a direct impact on ICT SCRM.

Table 2-1: Supply Chain Risk Management Stakeholders

Tiers	Tier Name	Generic Stakeholder	Activities
1	Organization	Executive Leadership (CEO, CIO, COO, CFO, CISO, CTO, etc.) - Risk executive	Corporate Strategy, Policy, goals and strategies

Tiers	Tier Name	Generic Stakeholder	Activities
2	Mission	Business Management (includes program management (PM), research and development (R&D), Engineering [SDLC oversight], Acquisitions / Procurement, Cost Accounting, -“ility” management [reliability, safety, quality], etc.)	Actionable Policies and procedures, Guidance and constraints
3	Operation	Systems Management (architect, developers, QA/QC, test, contracting personnel (approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, etc.)	Policy implementation Requirements, constraints implementations

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

The next few sections provide example activities in each tier. However, because each organization is different, there may be activities that are performed in different tiers as individual organizational context requires.

2.1.1 TIER 1 – ORGANIZATION

Tier 1 (Organization) provides strategic direction through organizational-level mission/business requirements and policies, establishing governance structures such as the risk xxecutive (function), and developing organization-wide investment strategies for ICT SCRM. Tier 1 activities help to ensure that ICT SCRM solutions are cost-effective, efficient, and consistent with the strategic goals and objectives of the organization. It is critical that in this tier, as Organizations define and implement organization-wide strategies, policies and processes, they include ICT SCRM considerations.

ICT SCRM activities at this tier include:

- Establish ICT SCRM policy based on external and organizational requirements and constraints (e.g., applicable laws and regulations) to include the purpose and applicability, as well as investment / funding requirements, of the ICT SCRM program;
- Based on the ICT SCRM policy, identify:
    - Mission/business requirements that will influence ICT SCRM, such as cost, schedule, performance, security, privacy, quality, and safety;

    - Information security requirements, including ICT SCRM-specific requirements; and
    - Organization-wide business/mission functions and how ICT SCRM will be integrated into these processes;
- Establish risk tolerance for ICT supply chain risks; and
- Establish ICT SCRM team for the organization.

Chapter 3 provides a number of organizational ICT SCRM controls that federal agency acquirers can tailor for their use to help guide Tier 1 ICT SCRM activities.

2.1.2 TIER 2 – MISSION/BUSINESS PROCESS

In Tier 2 (Mission/Business Process), risk is addressed by designing, developing, and implementing mission/business processes that support the missions/business functions defined at Tier 1. In this tier, program requirements are defined and managed – including cost, schedule, performance, and a variety of critical nonfunctional requirements, including ICT SCRM. These nonfunctional requirements are also known as "ilities" and include concepts such as reliability, dependability, safety, and quality. Many threats *to* and *through* the supply chain are addressed at this level in the management of trust relationships with system integrators and suppliers of ICT products and services. Because ICT SCRM can both directly and indirectly impact mission/business processes, understanding the intersections and integrating and coordinating ICT SCRM activities at this tier is critical for ensuring successful federal agency mission and business operations.

ICT SCRM activities at this tier include:

- Defining the risk response strategy, including ICT SCRM considerations, for critical processes;
- Establishing ICT SCRM processes to support mission / business functions;
- Determining the ICT SCRM requirements of the mission/business systems needed to execute the mission/business processes;
- Incorporating ICT SCRM requirements into the mission/business processes;
- Integrating ICT SCRM requirements into an enterprise architecture to facilitate the allocation of ICT SCRM controls to organizational information systems and the environments in which those systems operate; and
- Establishing a mission/business-specific ICT SCRM team that coordinates and collaborates with the organizational ICT SCRM team.

Chapter 3 provides a number of mission/business ICT SCRM controls that Organizations can tailor for their use to help guide Tier 2 ICT SCRM activities.

2.1.3 TIER 3 – INFORMATION SYSTEMS

Tier 3 (Information Systems) is where ICT SCRM activities are integrated into the SDLC of organizational information systems and system components. Many threats *through* the supply chain are addressed at this level through the use of ICT SCRM-related information security requirements. Risk management activities at Tier 3 reflect the organization's risk management strategy defined in Tier 1, as well as cost, schedule, and performance requirements for individual information systems as defined in Tier 2. ICT SCRM activities at this tier include:

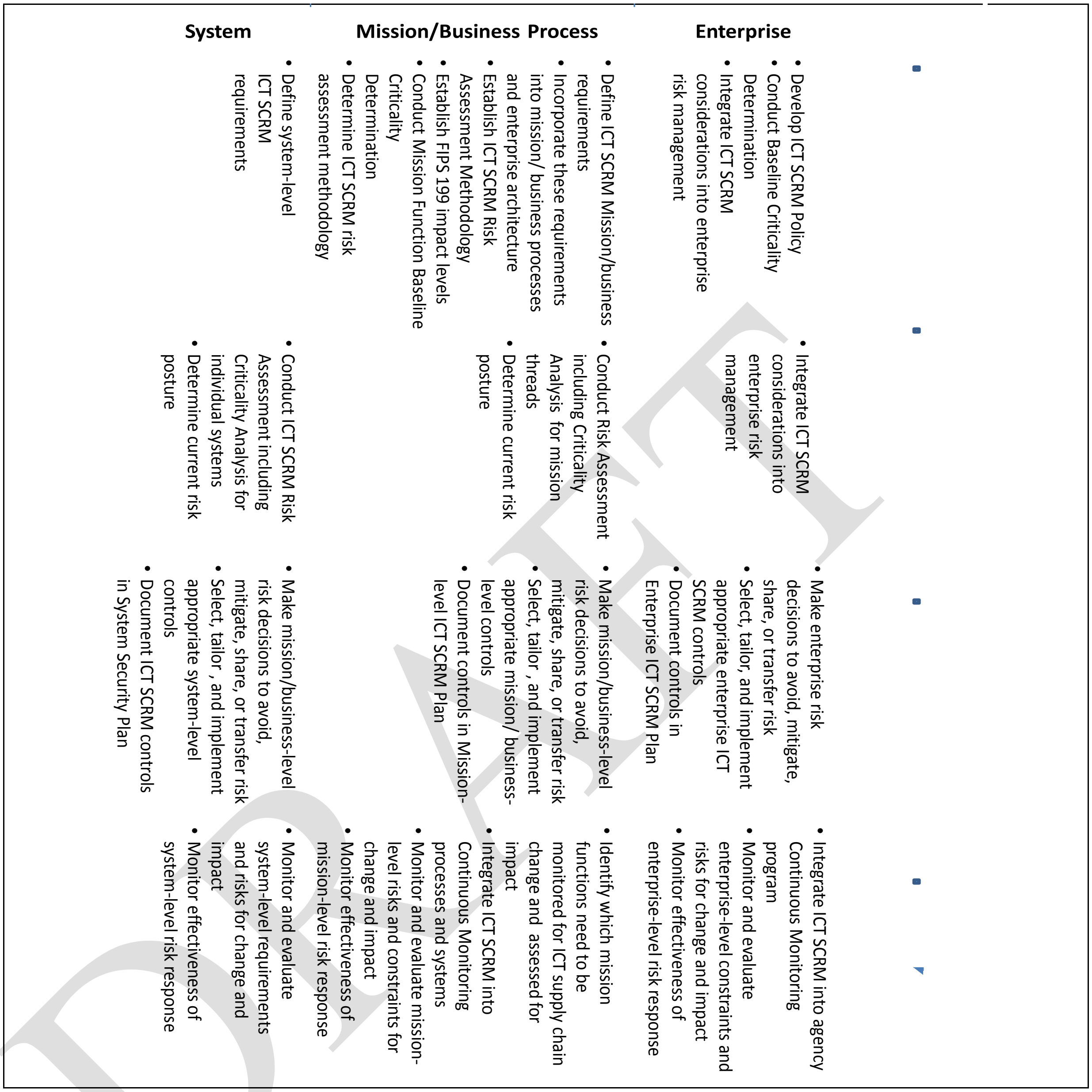
- Applying ICT SCRM controls in the development and sustainment of systems supporting mission/business processes; and
- Applying ICT SCRM controls to the SDLC and the environment in which the SDLC is conducted (e.g., development environment) (including ICT components and processes) used to develop and integrate mission/business systems.

At Tier 3, ICT SCRM significantly intersects with the SDLC which includes acquisition (both custom and off-the-shelf), requirements, architectural design, development, delivery, installation, integration, maintenance, and disposal/retirement of information systems, including ICT products and services.

2.2 ICT SCRM ACTIVITIES IN RISK MANAGEMENT PROCESS

The steps in the risk management process – Frame, Assess, Respond, and Monitor - are not inherently sequential in nature. The steps are performed in different ways, depending on the particular tier where the step is applied on prior activities related to each of the steps. Organizations have significant flexibility in how the risk management steps are performed (e.g., sequence, degree of rigor, formality, and thoroughness of application) and in how the results of each step are captured and shared—both internally and externally. What is consistent is that the outputs or post conditions from a particular risk management step directly impact one or more of the other risk management steps in the risk management process.

Figure 2-3 summarizes ICT SCRM activities throughout the risk management process as they are performed within the three organizational tiers. The arrows between different steps of the risk management process depict simultaneous flow of information and guidance among the steps. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.



Enterprise	• Develop ICT SCRM Policy • Conduct Baseline Criticality Determination • Integrate ICT SCRM considerations into enterprise risk management	• Integrate ICT SCRM considerations into enterprise risk management	• Make enterprise risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor, and implement appropriate enterprise ICT SCRM controls • Document controls in Enterprise ICT SCRM Plan	• Integrate ICT SCRM into agency Continuous Monitoring program • Monitor and evaluate enterprise-level constraints and risks for change and impact • Monitor effectiveness of enterprise-level risk response
Mission/Business Process	• Define ICT SCRM Mission/business requirements • Incorporate these requirements into mission/ business processes and enterprise architecture • Establish ICT SCRM Risk Assessment Methodology • Establish FIPS 199 impact levels • Conduct Mission Function Baseline Criticality Determination • Determine ICT SCRM risk assessment methodology	• Conduct Risk Assessment including Criticality Analysis for mission threads • Determine current risk posture	• Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor , and implement appropriate mission/ business-level controls • Document controls in Mission-level ICT SCRM Plan	• Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact • Integrate ICT SCRM into Continuous Monitoring processes and systems • Monitor and evaluate mission-level risks and constraints for change and impact • Monitor effectiveness of mission-level risk response
System	• Define system-level ICT SCRM requirements	• Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems • Determine current risk posture	• Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk • Select, tailor , and implement appropriate system-level controls • Document ICT SCRM controls in System Security Plan	• Monitor and evaluate system-level requirements and risks for change and impact • Monitor effectiveness of system-level risk response

Figure 2-3. ICT SCRM Activities in Risk Management Process

Figure 2-4 depicts the order in which each analysis is executed and the interactions required to ensure that the analysis is inclusive of the various inputs at the organization, mission, and operations levels.

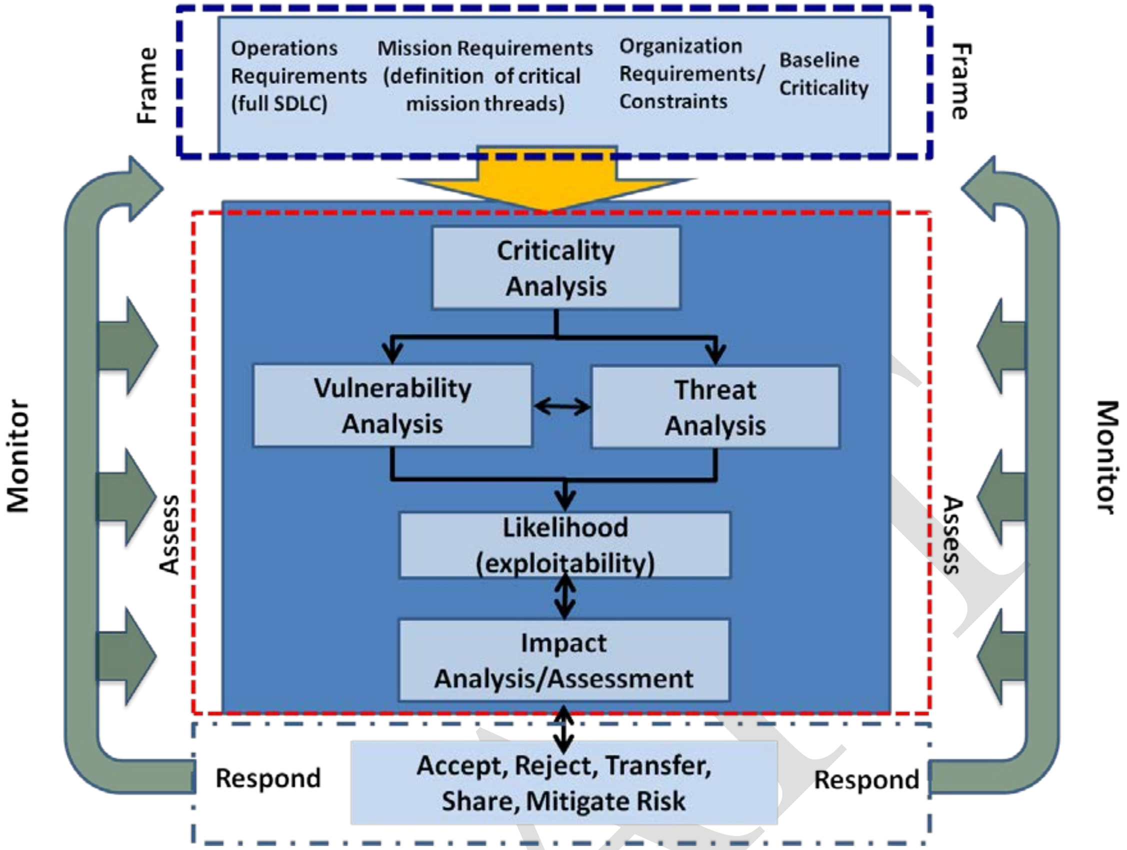

Frame
Operations Requirements (full SDLC)
Mission Requirements (definition of critical mission threads)
Organization Requirements/ Constraints
Baseline Criticality
Frame
Monitor
Assess
Criticality Analysis
Vulnerability Analysis
Threat Analysis
Likelihood (exploitability)
Impact Analysis/Assessment
Assess
Monitor
Respond
Accept, Reject, Transfer, Share, Mitigate Risk
Respond

Figure 2-4. ICT SCRM Risk Assessment

The remainder of this section provides a detailed description of ICT SCRM activities within the Frame, Assess, Respond, and Monitor steps of the Risk Management Process.

2.2.1 FRAME

Inputs and Preconditions

Frame is the step that establishes context for ICT SCRM in all three tiers. The scope and structure of the organizational ICT supply chain landscape, the overall risk management strategy, as well as specific program/project or individual information system needs, are defined in this step. The data and information collected during Frame provides inputs for scoping and fine-tuning ICT SCRM activities in other risk management process steps throughout the three tiers.

NIST SP 800-39 defines risk framing as “the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization’s approach for managing risk.” ICT SCRM risk framing should be integrated into the overall enterprise risk framing process. Outputs of the organization’s risk framing and the overall risk management process should serve as inputs into the ICT SCRM risk framing, including but not limited to:

- Enterprise policies, strategies, governance;
- Applicable laws and regulations;

- Mission functions and business goals;
- Enterprise processes (security, quality, etc.);
- Enterprise threats, vulnerabilities, risks, risk tolerance;
- Criticality of mission functions;
- Enterprise Architecture;
- Mission-level security policies;
- Functional requirements; and
- Security requirements.

ICT SCRM risk framing is an iterative process that also uses inputs from the other steps of the risk management process (assess, respond, monitor) as inputs. Figure 2-5 depicts the Frame Step with its inputs and outputs along the three organizational tiers.

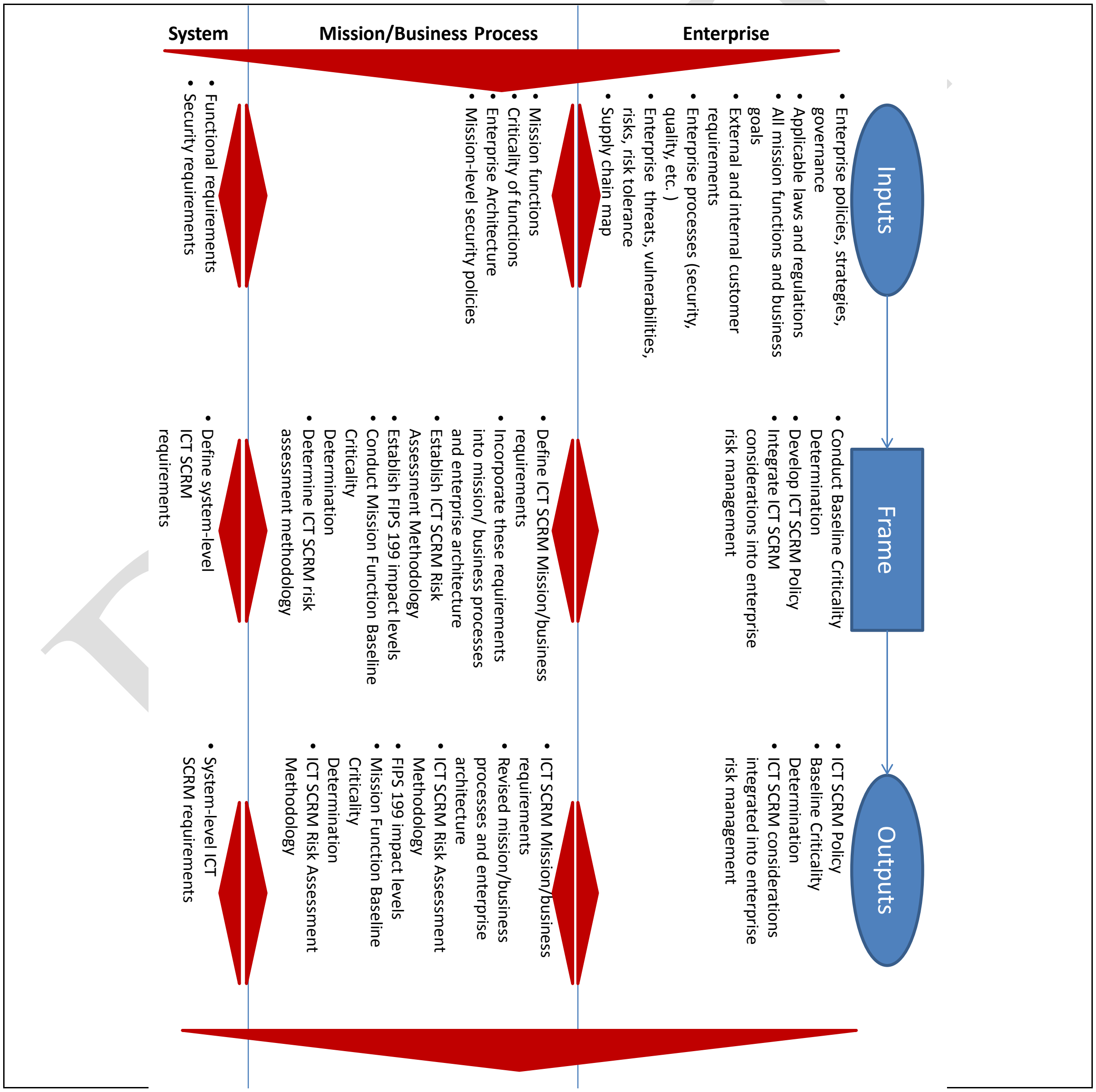

System
Mission/Business Process
Enterprise
Inputs
• Enterprise policies, strategies, governance
• Applicable laws and regulations
• All mission functions and business goals
• External and internal customer requirements
• Enterprise processes (security, quality, etc.)
• Enterprise threats, vulnerabilities, risks, risk tolerance
• Supply chain map
• Mission functions
• Criticality of functions
• Enterprise Architecture
• Mission-level security policies
• Functional requirements
• Security requirements
Frame
• Conduct Baseline Criticality Determination
• Develop ICT SCRM Policy
• Integrate ICT SCRM considerations into enterprise risk management
• Define ICT SCRM Mission/business requirements
• Incorporate these requirements into mission/ business processes and enterprise architecture
• Establish ICT SCRM Risk Assessment Methodology
• Establish FIPS 199 impact levels
• Conduct Mission Function Baseline Criticality Determination
• Determine ICT SCRM risk assessment methodology
• Define system-level ICT SCRM requirements
Outputs
• ICT SCRM Policy
• Baseline Criticality Determination
• ICT SCRM considerations integrated into enterprise risk management
• ICT SCRM Mission/business requirements
• Revised mission/business processes and enterprise architecture
• ICT SCRM Risk Assessment Methodology
• FIPS 199 impact levels
• Mission Function Baseline Criticality Determination
• ICT SCRM Risk Assessment Methodology
• System-level ICT SCRM requirements

Figure 2-5. ICT SCRM in the Frame Step

Figure 2-5 depicts inputs, activities, and outputs of the Frame Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Frame Step include inputs from other steps as well as inputs from the enterprise risk management process that are shaping the ICT SCRM process. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Activities

RISK ASSUMPTIONS

TASK 1-1: Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization.

Supplemental Guidance:

As a part of identifying ICT supply chain Risk Assumptions within the broader Risk Management process (described in NIST SP 800-39), agencies should do the following:

- Define ICT SCRM mission, business, and system-level requirements;
- Identify which mission functions and related components are critical to the organization, including FIPS 199 impact level, to determine the baseline criticality;
- Identify, characterize, and provide representative examples of threat sources, vulnerabilities, consequences/impacts, and likelihood determinations related to ICT supply chain;
- Develop enterprise-wide ICT SCRM policy;
- Select appropriate ICT supply chain risk assessment methodologies, depending on organizational governance, culture, and diversity of the missions/business functions; and
- Establish a method for the results of ICT SCRM activities to be integrated into the overall agency Risk Management Process.

Baseline Criticality:

Federal agencies should define the baseline criticality in the Frame phase to facilitate performance of the criticality analysis in the Assess phase. Baseline criticality is the initial identification of those components and processes that are critical for the particular system based on system function. This includes the analysis of requirements, architecture, and design to identify the minimum set of components required for system operation. Baseline criticality determination includes first identifying system requirements to support mission function and systems/components that have a direct impact on system requirements. This analysis should include agency system and ICT supply chain dependencies and access to the ICT supply chain.

Baseline criticality is performed at Tier 3 but has implications to Tiers 1 and 2 in terms of the impact of ICT supply chain compromise on organizational (Tier 1) and mission (Tier 2) activities supported by the system that includes those specific critical components. Therefore Tiers 1 and 2 should influence the determination of the baseline criticality as indicated in the following specific steps involved in determining baseline criticality:

- Identify mission and business drivers, such as applicable regulations, policies, requirements, and operational constraints;
- Identify, group, and prioritize mission functions based on the drivers;
- Map the mission functions to the system architecture and identify the systems/ components (hardware, software, and firmware) and processes that are critical to the mission/business effectiveness of the system or an interfacing network;
- Perform a dependency analysis and assessment to establish which components may require hardening given the system architecture;
- Review the existing supply chain map[10] for critical systems and components to identify additional considerations for baseline criticality determination; and
- Allocate criticality levels (high, medium, low) to the identified systems/components and establish FIPS 199 impact levels for individual systems.

Please note that baseline criticality can be determined for existing systems or for future system integration efforts based on system architecture and design. It is an iterative activity that should be performed if a change warranting iteration is identified in Monitor.

Threat Sources:

For ICT SCRM, threat sources include: (i) hostile cyber/physical attacks either to the supply chain or to an information system component(s) traversing the supply chain; (ii) human errors; or (iii) political unrest, natural, or man-made disasters. NIST SP 800-39 states that organizations provide a succinct characterization of the types of tactics, techniques, and procedures employed by adversaries that are to be addressed by safeguards and countermeasures (i.e., security controls) deployed at Tier 1 (organization level), at Tier 2 (mission/business process level), and at Tier 3 (information system level)—making explicit the types of threat-sources that are to be addressed as well as making explicit those not being addressed by the safeguards/countermeasures.

Threat information may come from multiple sources, including partners, suppliers, and customers. Supply chain maps can be valuable threat information sources and may be obtained from supply chain and logistics professionals within an agency. A supply chain map is a visual and verbal depiction of how critical components (software and hardware) traverse logical and physical space. The information that provides inputs into the supply chain map includes historical data, results of qualitative analysis, and open or all-source information.

The supply chain map provides the context for identifying possible locations or access points for thereat agents to enter the ICT supply chain. The ICT supply chain threat agents are similar to the information security threat agents, such as attackers or industrial spies. Table 2-4 lists examples of ICT supply chain threat agents. Appendix F provides Supply Chain Threat Scenarios listed in Table 2-4.

Table 2-4. Example ICT Supply Chain Threat Agents

Threat Agent	Scenario	Examples
Counterfeiters	Counterfeits	Criminal groups seek to acquire and sell counterfeit ICT

[10] Supply chain map is a description or depiction of supply chain including its nodes, locations, and delivery paths, both physical and logical.

Threat Agent	Scenario	Examples
	inserted into ICT supply chain (see Appendix F Scenario 1)	components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain ICT components that they can sell through various gray market resellers to acquirers.[11]
Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation.[12]
Foreign Intelligence Services	Malicious code insertion (see Appendix F Scenario 3)	Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) to be used when the system is operational to gather information or subvert system or mission operations.
Terrorists	Unauthorized access	Terrorists seek to penetrate ICT supply chain and may implant unwanted functionality (by inserting new or modifying existing functionality) or subvert system or mission operations.
Industrial Espionage	Industrial Espionage (see Appendix F Scenario 2)	Industrial spies seek to penetrate ICT supply chain to gather information or subvert system or mission operations.

Agencies can identify and refine ICT SCRM-specific threats in all three tiers. Table 2-5 provides examples of threat considerations and different methods that can be used to characterize ICT supply chain threats at different tiers.

Table 2-5. Supply Chain Threat Considerations

Tier	Threat Consideration	Methods
Tier 1	• Organization’s business and mission • Strategic supplier relationships • Geographical considerations related to the extent of the organization’s ICT supply chain	• Establish common starting points for identifying ICT supply chain threat. • Establish procedures for countering organization-wide threats such as natural disasters.
Tier 2	• Mission functions • Geographic locations • Types of suppliers (COTS, external service providers, or custom, etc.) • Technologies used enterprise-wide	• Identify additional sources of threat information specific to organizational mission functions. • Identify potential threat sources based on the locations and suppliers identified through examining the agency supply chain map.

[11] “Defense Industrial Base Assessment: Counterfeit Electronics,” U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010=

[12] Reference published cases of such events.

Tier	Threat Consideration	Methods
		• Scope identified threat sources to the specific mission functions, using the supply chain maps. • Establish mission-specific preparatory procedures for countering threat adversaries/natural disasters.
Tier 3	• SDLC	• Consider the phase in the system development life cycle to determine the level of detail with which threats should be considered. • Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.

Vulnerabilities

Organizations should identify approaches used to characterize ICT supply chain vulnerabilities, consistent with the characterization of threat sources and events and with the overall approach for characterizing vulnerabilities used by the organization. Appendix E provides examples of ICT supply chain threat events, based on NIST SP 800-30 Rev1 Appendix E.

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.[13] Within the ICT SCRM context, it is any weakness in the system/component design, development, manufacturing, production, shipping and receiving, delivery, or operation that can be exploited by a threat agent to significantly degrade performance of a system that supports the mission.

ICT supply chain vulnerabilities may be found in:

- The systems/components within the SDLC (i.e., being developed and integrated);
- The development and operational environment directly impacting the SDLC; and
- The logistics / delivery environment that transports ICT systems and components (logically or physically).

All three tiers should contribute to determining the approaches to characterize vulnerabilities, with progressively more detail identified and documented in the lower tiers. Table 2-6 provides examples of considerations and different methods that could be used to characterize ICT supply chain vulnerabilities at different tiers.

Table 2-6. Supply Chain Vulnerabilities Considerations

Tier	Vulnerability Consideration	Methods
Tier 1	• Organization’s business and mission	• Examine agency Supply Chain Maps

[13] SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200

Tier	Vulnerability Consideration	Methods
	• Supplier relationships (e.g., system integrators, COTS, external services) • Geographical considerations related to the extent of the organization’s ICT supply chain • Enterprise / Security Architecture • Criticality Baseline	and/or historical data to identify especially vulnerable locations or organizations. • Analyze agency mission for susceptibility to potential supply chain vulnerabilities. • Examine system integrator and supplier relationships for susceptibility to potential supply chain vulnerabilities. • Review enterprise architecture and criticality baseline to identify areas of weakness requiring more robust ICT supply chain considerations.
Tier 2	• Mission functions • Geographic locations • Types of suppliers (COTS, custom, etc.) • Technologies used	• Refine analysis from Tier 1 based on specific mission functions and applicable threat and supply chain information. • Consider using CVEs to characterize and categorize vulnerabilities. • Consider using scoring guidance to prioritize vulnerabilities for remediation.
Tier 3	• Individual technologies, solutions, and suppliers should be considered	• Use CVEs where available to characterize and categorize vulnerabilities • Identify weaknesses

Consequences and Impact

For ICT SCRM, impact is always in relation to the acquirer’s mission and includes the systems or components traversing through the supply chain as well as the supply chain itself. Potential impacts can be gathered through reviewing historical data for the agency, similar peer organizations, or applicable industry surveys.

The following are examples of ICT supply chain consequences and impact:

- An earthquake in Malaysia reduced the number of commodity DRAMs to 60% of the world’s supply, creating a shortage for hardware maintenance and new design.
- Accidental procurement of a counterfeit part resulted in premature component failure, therefore impacting organization’s mission performance.

Likelihood

In Information Assurance risk analysis, likelihood is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.[14]

[14] CNSSI-4009

Agencies should determine which approaches they are going to use to determine the likelihood of ICT supply chain compromise, consistent with the overall approached used by the agency risk management function.

RISK CONSTRAINTS

TASK 1-2: Identify constraints[15] on the conduct of risk assessment, risk response, and risk monitoring activities within the organization.

Supplemental Guidance:

Identify the following two types of constraints to ensure that ICT supply chain is integrated into the agency risk management process:

1. Agency constraints; and
2. ICT supply chain-specific constraints.

Agency constraints serve as an overall input into framing the ICT supply chain policy at Tier 1, mission requirements at Tier 2, and system-specific requirements at Tier 3. Table 2-7 lists the specific agency and ICT supply chain constraints. ICT supply chain constraints, such as ICT SCRM policy and ICT SCRM requirements, may need to be developed if they do not exist.

Table 2-7. Supply Chain Constraints

Tier	Agency Constraint	ICT Supply Chain Constraint
Tier 1	• Enterprise policies, strategies, governance • Applicable laws and regulations • Mission functions • Enterprise processes (security, quality, etc.)	• Develop enterprise ICT SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission functions; and enterprise processes.
Tier 2	• Mission functions • Criticality of functions • Enterprise Architecture • Mission-level security policies	• Define ICT SCRM Mission/business requirements. • Incorporate these requirements into mission/ business processes and enterprise architecture.
Tier 3	• Functional requirements • Security requirements	• Define system-level ICT SCRM requirements.

An enterprise ICT SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable enterprise policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with the internal and external

[15] Refer to NIST SP 800-39, Section 3.1, Task 1-2 for a description of constraints in the risk management context.

customer requirements. It should also define the integration points for ICT SCRM with the agency Risk Management Process and with agency SDLC.

ICT SCRM policy should define ICT SCRM-related roles and responsibilities of the agency ICT SCRM team, any dependencies among those roles, and the interaction among the roles. ICT SCRM-related roles will articulate responsibilities for conducting the risk assessment, applying the mitigations to implement risk-based decision, and performing monitoring. Identifying and validating roles will also help to specify the amount of effort that will be required to implement the ICT SCRM Plan. Examples of ICT SCRM-related roles include:

- Risk executive function that provides overarching ICT supply chain risk guidance to engineering decisions that specify and select ICT products as the system design is finalized;
- Procurement officer and maintenance engineering responsible for identifying and replacing the hardware when defective;
- Delivery organization and acceptance engineers who verify that the part is acceptable to receive into the acquiring organization;
- System integrator responsible for system maintenance and upgrades, whose staff resides in the acquirer facility and uses system integrator development infrastructure and the acquirer operational infrastructure; and
- The end user of ICT systems/components/services.

ICT SCRM requirements should be guided by the ICT SCRM policy, as well as mission functions and their criticality at Tier 2 and by known functional and security requirements at Tier 3.

RISK TOLERANCE

TASK 1-3: Identify the level of risk tolerance for the organization.

Supplemental Guidance:

Risk tolerance is the level of risk that organizations are willing to accept in pursuit of strategic goals and objectives (NIST SP 800-39). Organizations should take into account ICT supply chain threats, vulnerabilities, constraints, and baseline criticality, when identifying the overall level of risk tolerance for their agencies.

PRIORITIES AND TRADE-OFFS

TASK 1-4: Identify priorities and trade-offs considered by the organization in managing risk.

Supplemental Guidance

As a part of identifying priorities and trade-offs, organizations should consider ICT supply chain threats, vulnerabilities, constraints, and baseline criticality.

Outputs and Post Conditions

Within the scope of NIST SP 800-39, “the output of the risk framing step is the *risk management strategy* that identifies how organizations intend to assess, respond to, and monitor risk over time. This strategy should clearly include ICT SCRM considerations that were identified and result in the establishment of ICT SCRM-specific processes throughout the agency. These processes should be documented in one of three ways:

1. Integrated into existing agency documentation;
2. A separate set of documents addressing ICT SCRM; or
3. A mix of separate and integrated documents, based on agency needs and operations.

The following information should be provided as an output of the risk framing step, regardless of how the outputs are documented:

- ICT SCRM Policy;
- Baseline Criticality Determination including prioritized mission functions and FIPS 199 criticality determination;
- ICT supply chain risk assessment methodology and guidance;
- ICT supply chain risk response guidance;
- ICT supply chain risk monitoring guidance;
- ICT SCRM mission/business requirements;
- Revised mission/business processes and enterprise architecture with ICT SCRM considerations integrated; and
- System-level ICT SCRM requirements.

Outputs from the risk framing step serve as inputs to the risk assessment, risk response, and risk monitoring steps.

2.2.2 ASSESS

Inputs and Preconditions

Assess is the step where all the collected data is used to conduct a risk assessment. A number of inputs are combined and analyzed to identify the likelihood and the impact of an ICT supply chain compromise, including criticality, threat, and vulnerability analysis results; stakeholder knowledge; and policy, constraints, and requirements.

ICT supply chain risk assessment should be integrated to the overall enterprise risk assessment processes throughout the organization. ICT SCRM risk assessment results should be used and aggregated as appropriate to communicate ICT supply chain risks at each tier of the organizational hierarchy. Figure 2-6 depicts the Assess Step with its inputs and outputs along the three organizational tiers.

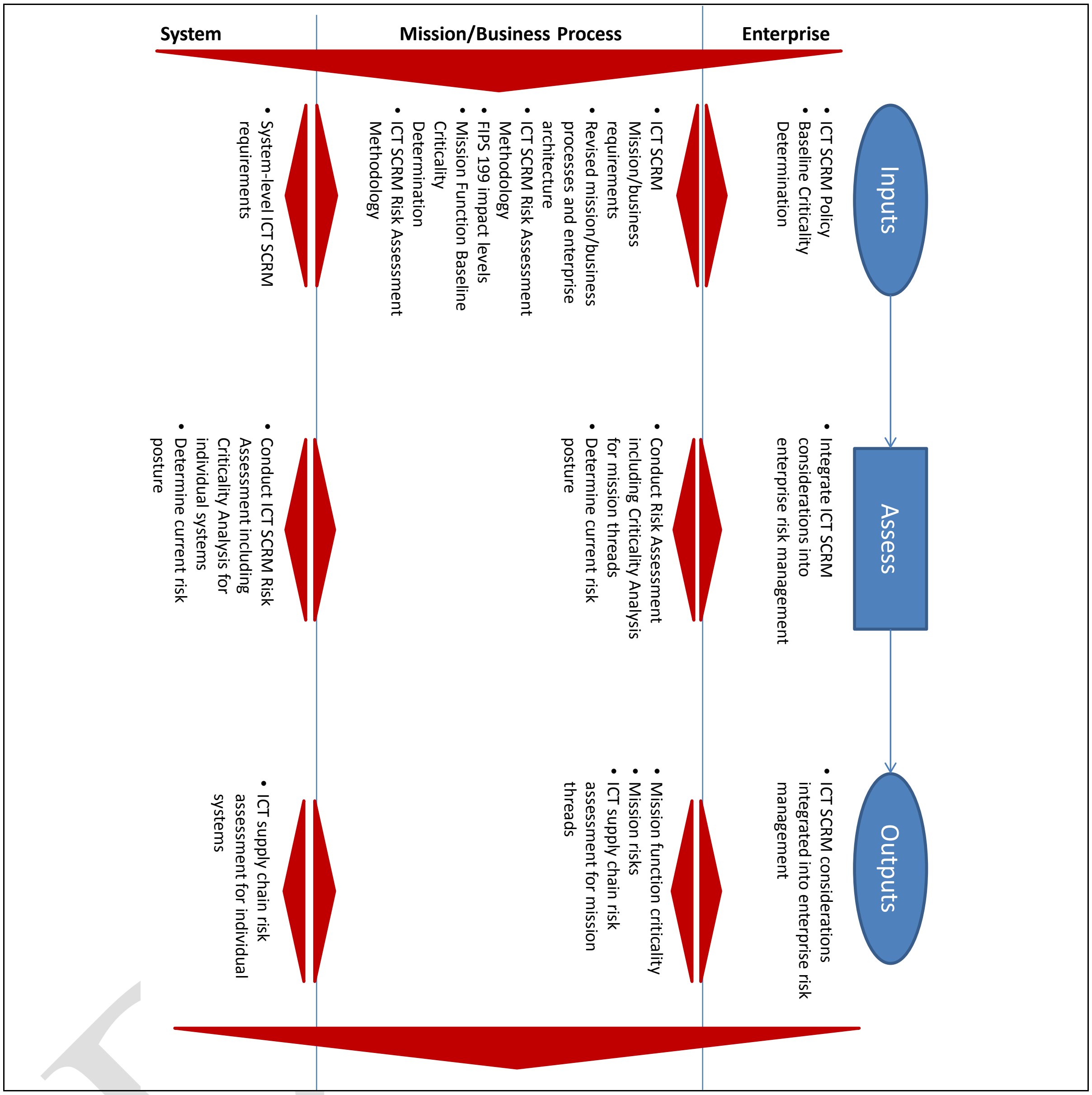

System
Mission/Business Process
Enterprise
Inputs
Assess
Outputs
• ICT SCRM Policy
• Baseline Criticality Determination
• ICT SCRM Mission/business requirements
• Revised mission/business processes and enterprise architecture
• ICT SCRM Risk Assessment Methodology
• FIPS 199 impact levels
• Mission Function Baseline Criticality Determination
• ICT SCRM Risk Assessment Methodology
• System-level ICT SCRM requirements
• Integrate ICT SCRM considerations into enterprise risk management
• Conduct Risk Assessment including Criticality Analysis for mission threads
• Determine current risk posture
• Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems
• Determine current risk posture
• ICT SCRM considerations integrated into enterprise risk management
• Mission function criticality
• Mission risks
• ICT supply chain risk assessment for mission threads
• ICT supply chain risk assessment for individual systems

Figure 2-6. ICT SCRM in the Assess Step

Similar to Figure 2-5, Figure 2-6 depicts inputs, activities, and outputs of the Assess Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Assess Step include inputs from the other steps. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Criticality, vulnerability, and threat analysis are critical components of the supply chain risk assessment process. As depicted in Figure 2-4, vulnerability and threat analysis can be performed in any order and may be performed iteratively to ensure that all applicable threats and vulnerabilities have been identified.

The order of activities that begins with the criticality analysis ensures that the assessment is scoped to include only relevant critical mission functions and the impact of ICT supply chain on these mission functions. The likelihood of exploitability is a key step to understanding impact. It becomes a synthesis point for criticality analysis, vulnerability analysis, and threat analysis and helps to further clarify impact to support an efficient and cost-effective risk decision

Activities

CRITICALITY ANALYSIS

TASK 2-0: Conduct Criticality Analysis of mission-critical functions, systems, and components to narrow the scope (and resources) for ICT SCRM activities on the issues that matter most to mission success.

Supplemental Guidance

Criticality analysis should include the ICT supply chain environment for both the federal agency and applicable suppliers and the systems/components/services. Criticality analysis assesses the direct impact they each have on the mission priorities. ICT supply chain environment includes the SDLC for applicable systems, services, and components because the SDLC defines whether security considerations are built into the systems/components or added after systems/components have been created.

Organizations should use Baseline Criticality Determination conducted during the Frame Step of the risk management process, including FIPS 199 system categorization, as a starting point for the criticality analysis. Once this determination is made, criticality analysis can be completed for the identified systems. Organizations should use their own discretion for whether to perform criticality analysis for moderate-impact systems.

The outcome of the criticality analysis is a narrowed, prioritized list of the organization's critical functions, systems, and components. Critical functions are those functions, which if corrupted or disabled, are likely to result in mission degradation or failure. Critical mission functions are dependent on their supporting systems that in turn depend on critical components in those systems system (hardware, software, and firmware). Mission-critical functions also depend on processes that are used to implement the critical functions. Those components and processes that deliver defensive functions (e.g., access control, identity management, crypto) and unmediated access (e.g., power supply) may also be considered mission-critical.

Criticality analysis is the primary method by which mission-critical functions and associated systems/components are identified and prioritized. Criticality analysis includes the following iterative steps:

- Identify organization's mission and business drivers, such as applicable regulations, policies, requirements, and operational constraints;

- Prioritize these drivers to help articulate the organization’s critical functions, systems, and components;
- Identify and group critical mission functions based on the drivers;
- Map the mission-critical functions to the system architecture and identify the systems/ components/services (hardware, software, and firmware) and processes that are critical to the mission/business effectiveness of the system or an interfacing network;
- Allocate criticality levels (high, moderate, low) to the components/services that have been defined; and
- Correlate identified critical components /services to ICT supply chain maps, historical data, and SDLC to identify critical ICT supply chain paths.

When identifying critical functions and associated systems/components and assigning them criticality levels, consider the following:

- Logic-bearing components are especially susceptible to malicious alteration throughout the program life cycle;
- Functional breakdown is an effective method to identify functions, associated critical components, and supporting defensive functions;
- Dependency analysis is used to identify the functions on which critical functions depend (e.g., defensive functions such as digital signatures used in software patch acceptance). Those functions become critical functions themselves; and
- Identification of all access points to identify and limit unmediated access to critical function/components (e.g., least-privilege implementation).

The resulting list of critical functions are used along with the vulnerability analysis and threat analysis to determine the initial ICT SCRM risk as depicted in Figure 2-4. ICT supply chain countermeasures and mitigations can then be selected and implemented to reduce risk to acceptable levels.

Criticality analysis is performed iteratively. The first iteration is likely to identify critical functions and systems/components that have a direct impact on mission functions and may be performed concurrently at each tier. Successive iterations will include the criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies defined at each of the other tiers. Each iteration will refine the criticality analysis results and result in the addition of defensive functions. Several iterations are likely needed to establish or update the criticality analysis results. Criticality analysis can be performed at any point in the program life cycle.

THREAT AND VULNERABILITY IDENTIFICATION

TASK 2-1: Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.

Supplemental Guidance

In addition to threat and vulnerability identification, as described in NIST SP 800-39 and NIST SP 800-30, organizations should conduct ICT supply chain threat analysis and vulnerability analysis.

Threat Analysis

Threat analysis provides specific and timely threat characterization of the potential threat actors, natural disaster possibilities, as well as identified system integrators, suppliers, or external service providers,[16] to inform management, acquisition, engineering, and operational activities within an organization. Threat analysis can use a variety of information to assess potential threats, including open source, intelligence, and counterintelligence. Such threats may include suppliers, natural disasters, or adversaries. Organizations should use the threat sources defined during the Frame Step in threat analysis conducted during the Assess Step. Organizations should use the results of the threat analysis in the Assess Step to ultimately support supplier selection, alternative build or buy decisions, and development and selection of appropriate mitigations in the Respond Step. ICT supply chain threat analysis should be based on the results of the criticality analysis. Specific identified threats may include people, processes, technologies, or natural and man-made disasters.

ICT supply chain threat analysis should capture at least the following data:

- Changes to the systems/components or SDLC environment;
- Observation of ICT supply chain-related attacks while they are occurring;
- Incident data collected post ICT supply chain-related compromise;
- Observation of tactics, techniques, and procedures used in specific attacks, whether observed or collected using audit mechanisms; and
- Natural and man-made disasters before, during and after occurrence.

Vulnerability Analysis

Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (NIST SP 800-53). Within ICT SCRM context, it is any weakness in system/component design, development, production, or operation that can be exploited by a threat to defeat a system's mission objectives or to significantly degrade its performance.

This definition applies to both the systems/components being developed and integrated (i.e., within the SDLC) and to the development and operational environment that supports the SDLC, including any security mitigations and techniques, such as identity management or access control systems. Vulnerability analysis is an iterative process that informs risk assessment and countermeasure selection. The vulnerability analysis works alongside the threat analysis to help inform the impact analysis and to help scope and prioritize vulnerabilities to be mitigated.

[16] Please note that threat characterization of system integrators, suppliers, and external service providers may be benign.

Vulnerability analysis in the Assess Step should use the approaches used during the Frame Step to characterize ICT supply chain vulnerabilities. Vulnerability analysis should begin with identifying vulnerabilities that are applicable to mission-critical functions and systems/components identified by criticality analysis. Investigation of vulnerabilities may indicate the need to raise or at least reconsider the criticality levels of functions and components identified in earlier criticality analyses. Later iterations of vulnerability analysis may also identify additional threats, or opportunities for threats, that were not considered in earlier threat assessments.

Table 2-8 provides examples of applicable ICT supply chain vulnerabilities that can be observed within the three organizational tiers.

Table 2-8: Examples of ICT Supply Chain Vulnerabilities Mapped to the Organizational Tiers

	Vulnerability Types	Mitigation Types
Tier 1 – Organization	1) Deficiencies or weaknesses in organizational governance structures or processes such as a lack a strategic plan for ICT SCRM	1) Provide guidance on how to consider dependencies on external organizations as vulnerabilities. 2) Seek out alternate sources of new technology including building in-house.
Tier 2 – Mission/ Business	1) No operational process is in place for detecting counterfeits. 2) No budget was allocated for the implementation of a technical screening for acceptance testing of ICT components entering the SDLC as replacement parts. 3) Susceptibility to adverse issues from innovative technology supply sources (e.g., technology owned or managed by third parties is buggy).	1) Develop a program for detecting counterfeits and allocate appropriate budgets for putting in resources and training. 2) Allocate budget for acceptance testing – technical screening of components entering into SDLC .
Tier 3 – Operation	1) Discrepancy in system functions not meeting requirements, resulting in substantial impact to performance	2) Initiate engineering change to address functional discrepancy and test correction for performance impact.

The principal vulnerabilities to watch for are:

- Access paths within the supply chain that would allow malicious actors to gain information about the system and ultimately introduce components that could cause the system to fail at some later time ("components" here include hardware, software, and firmware);

- Access paths that would allow malicious actors to trigger a component malfunction or failure during system operations; and
- Dependencies on supporting or associated components that might be more accessible or easier for malicious actors to subvert than components that directly perform critical functions.

Factors to consider include the ease or difficulty of successfully attacking through a vulnerability and the ability to detect access used to introduce or trigger a vulnerability. The objective is to assess the net effect of the vulnerability, which will be combined with threat information to determine the likelihood of successful attacks in the risk assessment process.

RISK DETERMINATION

TASK 2-2: Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities.

Supplemental Guidance

Organizations determine ICT supply chain risk by considering the likelihood that known threats exploit known vulnerabilities to and through the ICT supply chain and the resulting consequences or adverse impacts (i.e., magnitude of harm) if such exploitations occur. Organizations use threat and vulnerability information together with likelihood and consequences/impact information to determine ICT SCRM risk either qualitatively or quantitatively.

Likelihood

Likelihood is the possibility of an exploit occurrence that may result in the loss of mission capability. It is defined as a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability (CNSSI-4009). Determining the likelihood requires the consideration of the characteristics of the threat sources, the identified vulnerabilities, and the organizations susceptibility to the ICT supply chain compromise, prior to and with the safeguards/mitigations implemented. This analysis should consider the degree of an adversary’s intent to interfere with federal agency acquirer’s mission. For example, how much time or money would the adversary spend to validate the existence of and leverage the vulnerability to attack a system? ICT supply chain risk assessment should consider two views:

- The likelihood that the ICT supply chain itself is compromised. This may impact, for example, the availability of quality components or increase the risk of IP theft.
- The likelihood that the system or component within the supply chain may be compromised. For example, if malicious code is inserted into a system or an electric storm damages a component. In some cases, these two views may overlap or be indistinguishable, but both may have an impact on the agency’s ability to perform its mission.

Likelihood determination should consider:

- Threat assumptions that articulate the types of threats that the system or the component may be subject to, such as cybersecurity threats, natural disasters, or physical security threats;
- Actual supply chain threat information such as adversaries' capabilities, tools, intentions, and targets;
- Exposure of components to external access;
- Identified system, process, or component vulnerabilities; and
- Empirical data on weaknesses and vulnerabilities available from any completed analysis (e.g., system analysis, process analysis) to determine probabilities of ICT supply chain threat occurrence.

The likelihood can be based on threat assumptions or actual threat data, such as previous breaches of the supply chain, specific adversary capability, historical breach trends, or frequency of breaches. The organization may use empirical data and statistical analysis to determine specific probabilities of breach occurrence, depending on the type of data available and accessible within the federal agency and from supporting organizations.

Impact

Impact is the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system (NIST SP 800-53 Rev4).

For ICT SCRM, impact includes the systems or components in the supply chain, the supply chain itself, and the organization- or mission-level activities. All three tiers in the risk management hierarchy may be impacted because ICT SCRM is an enterprise process.

Organizations should begin impact analysis with the potential impacts identified during the Frame Step, determining the *impact* of a compromise and then the impact of mitigating that compromise. Organizations need to identify the various adverse impacts of compromise, including: (i) the characteristics of the threat sources that could initiate the events; (ii) identified vulnerabilities; and (iii) the organizational susceptibility to such events based on planned or implemented countermeasures. Impact analysis is an iterative process performed initially when a compromise occurs, when mitigation approach is decided to evaluate the impact of change, and finally, in the ever changing SDLC, when the situation/context of the system or environment changes.

Organizations should use the result of impact analysis to define acceptable ICT supply chain risk posture for a given system. Impact is derived from criticality, threat, and vulnerability analyses results, and should be based on the likelihood of exploit occurrence. Impact is likely to be a qualitative measure requiring an analyst judgment. Impact is used by executive/decision maker as an input into the risk-based decisions whether to accept, avoid, mitigate, share, or transfer the resulting risks and the consequences of such decisions.

Organizations should document the overall results of ICT supply chain risk assessments in risk assessment reports.[17] ICT supply chain risk assessment reports should cover risks in all three organizational tiers as applicable. Based on the organizational structure and size, multiple ICT supply chain risk assessment reports may be required. Agencies are encouraged to develop individual reports at Tier 1. For Tier 2, agencies may want to integrate ICT supply chain risks into the respective mission-level Business Impact Assessments (BIA) or develop separate mission-level ICT supply chain risk assessment reports. For Tier 3, agencies may want to integrate ICT supply chain risks into the respective System Risk assessment Reports or develop separate system-level ICT supply chain risk assessment reports. ICT supply chain risk assessment report applies only to High Criticality systems per FIPS 199. Organizations may decide to develop ICT supply chain risk assessment reports for Moderate Criticality systems per FIPS 199.

ICT supply chain risk assessment reports at all three tiers should be interconnected and reference each other when appropriate.

Outputs and Post Conditions

This step results in:

- Confirmed mission function criticality;
- Establishment of relationships between the critical aspects of the system's ICT supply chain environment (e.g., SDLC) and applicable threats and vulnerabilities;
- Understanding of the likelihood and the impact of a potential ICT supply chain compromise;
- Understanding of mission and system-specific risks;
- Documented ICT supply chain risk assessments for mission functions and individual systems; and
- Integration of relevant ICT supply chain risk assessment results into the enterprise risk management process.

2.2.3 RESPOND

Inputs and Preconditions

Respond is the step in which the individuals conducting risk assessment will communicate the assessment results, proposed mitigation/controls options, and the corresponding risk posture for each proposed option to the decision makers. This information should be presented in a manner appropriate to inform and guide risk-based decisions. This will allow decision makers to finalize appropriate risk response based on the set of options along with the corresponding risk factors for choosing the various options.

[17] See NIST SP 800-30, Appendix K, for a description of risk assessment reports.

ICT supply chain risk response should be integrated into the overall enterprise risk response. Figure 2-7 depicts the Respond Step with its inputs and outputs along the three organizational tiers.

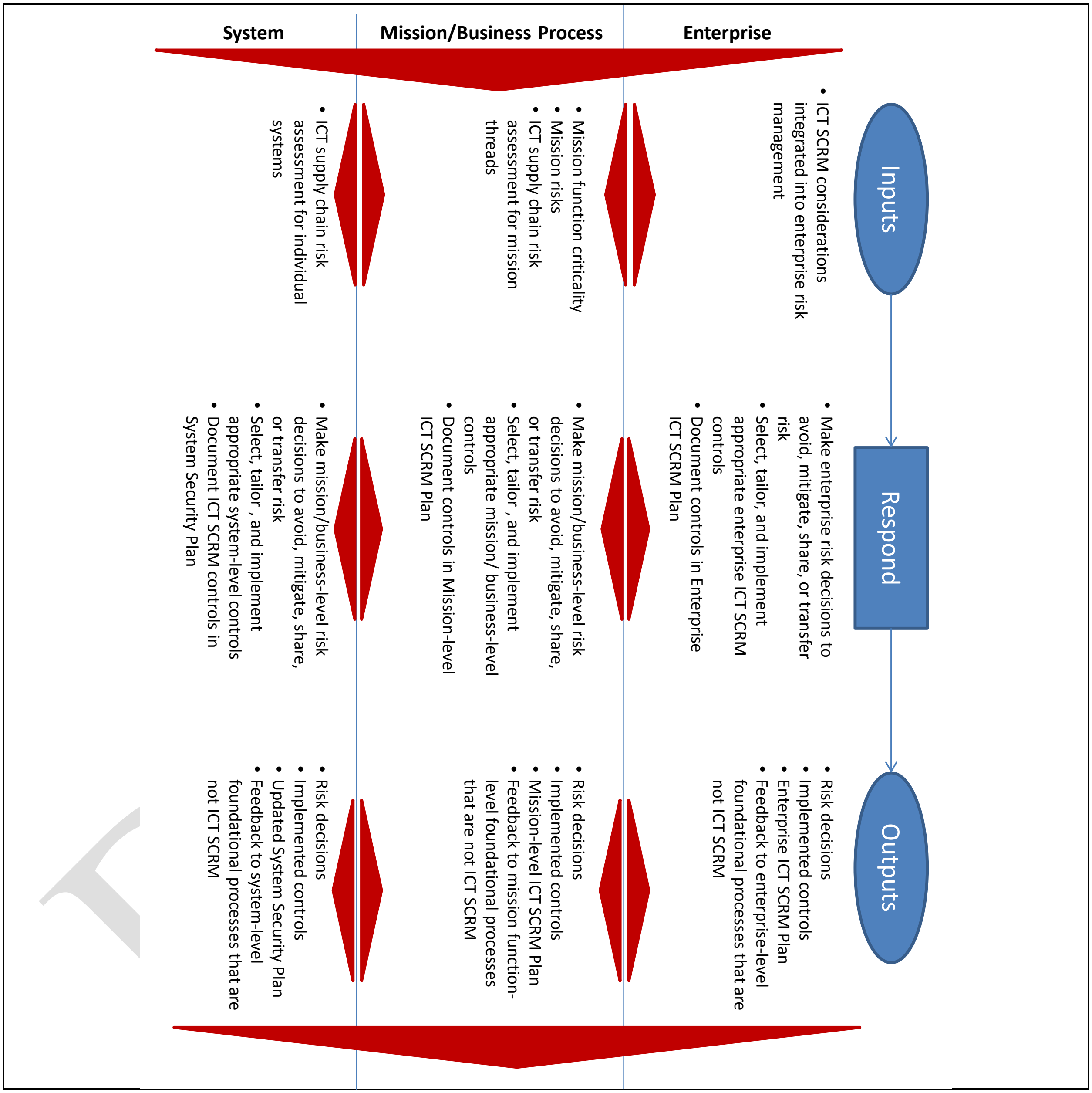

Enterprise
Mission/Business Process
System
Inputs
Respond
Outputs
ICT SCRM considerations integrated into enterprise risk management
Mission function criticality
Mission risks
ICT supply chain risk assessment for mission threads
ICT supply chain risk assessment for individual systems
Make enterprise risk decisions to avoid, mitigate, share, or transfer risk
Select, tailor, and implement appropriate enterprise ICT SCRM controls
Document controls in Enterprise ICT SCRM Plan
Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk
Select, tailor , and implement appropriate mission/ business-level controls
Document controls in Mission-level ICT SCRM Plan
Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk
Select, tailor , and implement appropriate system-level controls
Document ICT SCRM controls in System Security Plan
Risk decisions
Implemented controls
Enterprise ICT SCRM Plan
Feedback to enterprise-level foundational processes that are not ICT SCRM
Risk decisions
Implemented controls
Mission-level ICT SCRM Plan
Feedback to mission function-level foundational processes that are not ICT SCRM
Risk decisions
Implemented controls
Updated System Security Plan
Feedback to system-level foundational processes that are not ICT SCRM

Figure 2-7. ICT SCRM in the Respond Step

Similarly to Figures 2-4, and 2-5, Figure 2-7 depicts inputs, activities, and outputs of the Respond Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from the other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Respond Step include inputs from other steps. Outputs of the Respond Steps serve as inputs into the other steps, as well as inputs into the overall enterprise Risk Management Program at all three tiers. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Activities

RISK RESPONSE IDENTIFICATION

TASK 3-1: Identify alternative courses of action to respond to risk determined during the risk assessment.

Organizations should select ICT SCRM controls and tailor these controls based on the risk determination. ICT SCRM controls should be selected for all three organizational tiers, as appropriate per findings of the risk assessments for the tiers.

This process should begin with determining acceptable risk posture to support the evaluation of alternatives (also known as trade-off analysis).

EVALUATION OF ALTERNATIVES

TASK 3-2: Evaluate alternative courses of action for responding to risk.

Once an initial acceptable risk posture has been defined and options identified, these options should be identified and evaluated for achieving this risk posture by selecting mitigations from ICT SCRM controls and tailoring them to the acquirer's context. Chapter 3 provides risk mitigations and more information on how to select and tailor them.

This step involves conducting analysis of alternatives to select the proposed options for ICT SCRM mitigations/controls to be applied throughout the organization.

To tailor a set of ICT SCRM controls, the acquirer should perform ICT SCRM and mission-level trade-off analysis to achieve appropriate balance among ICT SCRM and functionality needs of the organization. This analysis will result in a set of cost-effective ICT SCRM controls that is dynamically updated to ensure that mission-related considerations trigger updates to ICT SCRM controls.

During this evaluation, applicable requirements and constraints are reviewed with the stakeholders, to ensure that ICT SCRM controls appropriately balance ICT SCRM and the broader organizational requirements, such as cost, schedule, performance, policy, and compliance.

ICT SCRM controls will vary depending on where they are applied within organizational tiers and SDLC processes. For example, ICT SCRM controls may range from using a blind buying strategy to obscure end use of a critical component, to design attributes (e.g., input validation, sandboxes, and anti-tamper design). For each implemented control, the Federal agency acquirer should identify someone responsible for its execution and develop a time- or event-phased plan for implementation throughout the SDLC. Multiple controls may address a wide range of possible risks. Therefore, understanding how the controls impact the overall risk is critical and must be considered before choosing and tailoring the combination of controls as yet another trade-off analysis may be needed before the controls can be finalized. The federal agency acquirer may be trading one risk for a larger risk unknowingly if the dependencies between the proposed controls and the overall risk are not understood and addressed.

RISK RESPONSE DECISION

TASK 3-3: Decide on the appropriate course of action for responding to risk.

As described in NIST SP 800-39, organizations should finalize identified and tailored ICT SCRM controls, based on the evaluation of alternatives and an overall understanding of threats, risks, and supply chain priorities.

Risk response decisions may be made by a risk executive or be delegated by the risk executive to someone else in the organization. While the decision can be delegated to Tier 2 or Tier 3, the significance and the reach of the impact should determine the tier where the decision is being made. Risk response decisions may be made in collaboration between federal agency risk executives, mission owners, and system owners, as appropriate.

The resulting decision, along with the selected and tailored controls should be documented in an ICT SCRM Plan. While the ICT SCRM Plan should ideally be developed proactively, it may also be developed in response to an ICT supply chain compromise. Ultimately, the ICT SCRM Plan should document an ICT SCRM baseline and identify ICT supply chain requirements and controls for Tiers 1, 2, and 3. The ICT SCRM Plan should be revised and updated based on the output of ICT supply chain monitoring.

The ICT SCRM Plan should cover activities in all three organizational tiers as applicable. Based on the organizational structure and size, multiple ICT SCRM plans may be required. Agencies are encouraged to develop individual plans at Tiers 1 and 2. For Tier 3, agencies may want to integrate ICT SCRM controls into the respective System Security Plans or develop separate system-level ICT SCRM Plans. At Tier 3, ICT SCRM Plan applies only to High Criticality systems per FIPS 199. Organizations may decide to develop an ICT SCRM Plan for Moderate Criticality systems per FIPS 199.

ICT SCRM Plans at all three tiers should be interconnected and reference each other when appropriate.

At each Tier, the plan should:

- Summarize the environment as determined in Frame such as applicable policies, processes, and procedures based on organization and mission requirements currently implemented in the organization;
- State the role responsible for the plan such as Risk Executive, CEO, CIO, Program Manager, System Owner;
- Identify key contributors such as CFO, COO, Acquisition/Contracting, System Engineer, Developer/Maintenance Engineer, Operations Manager, System Architect;
- Provide applicable (per tier) set of controls resulting from the Analysis of Alternatives (in Respond);
- Describe feedback processes among the tiers to ensure ICT supply chain interdependencies are addressed;
- Define frequency for deciding whether the plan needs to be revised; and
- Include criteria that would trigger revision.

Table 2-9 summarizes the controls to be contained in the ICT SCRM Plans at Tiers 1, 2, and 3 and provides examples of those controls.

Table 2-9. ICT SCRM Plan Controls at Tiers 1, 2, and 3

Tier	Controls	Examples
Tier 1	• Provides enterprise common controls baseline to Tiers 2 and 3	• Minimum sets of controls applicable to all ICT suppliers • Enterprise-level controls applied to processing and storing supplier information • ICT supply chain training and awareness for acquirer staff at the enterprise level
Tier 2	• Inherits common controls from Tier 1 • Provides mission function-level common controls baseline to Tier 3 • Provides feedback to Tier 1 about what is working and what needs to be changed	• Minimum sets of controls applicable to ICT suppliers for the specific mission function • Program level refinement of Identity and Access Management controls to address ICT SCRM concerns • Program-specific ICT supply chain training and awareness .

Tier 3	• Inherits common controls from Tiers 1 and 2 • Provides system-specific controls for Tier 3 • Provides feedback to Tier 2 and Tier 1 about what is working and what needs to be changed	• Minimum sets of controls applicable to specific hardware and software for the individual system • Appropriately rigorous acceptance criteria for change management for systems that support ICT supply chain, e.g., as testing or integrated development environments • System-specific ICT supply chain training and awareness • Intersections with the SDLC

RISK RESPONSE IMPLEMENTATION

TASK 3-4: Implement the course of action selected to respond to risk.

Organizations should implement the ICT SCRM Plan in a manner that integrates the ICT SCRM controls into the overall agency risk management processes.

Outputs and Post Conditions

The output of this step is a set of ICT SCRM controls that address ICT SCRM requirements and can be incorporated into the system requirements baseline. These requirements and resulting controls will be incorporated into the SDLC and other organizational processes, throughout the three tiers.

This step results in:

- Selected, evaluated, and tailored ICT SCRM controls that address potential compromise;
- Identified consequences of accepting or not accepting the proposed mitigations; and
- Development and implementation of the ICT SCRM Plan.

2.2.4 MONITOR

Inputs and Preconditions

Monitor is the step in which the project/program is routinely evaluated to maintain or adjust its risk posture. Changes to organization, mission/business, or operations can directly impact the risk posture of an individual project/program and of the organization's ICT supply chain processes. Monitor provides the mechanism for tracking such changes and ensuring they are appropriately assessed for impact (in Assess). Organizations should integrate ICT SCRM into existing continuous monitoring programs.[18] In case a Continuous Monitoring program does not exist, ICT SCRM can serve as a catalyst for establishment of a more comprehensive continuous monitoring

[18] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, describes how to establish and implement a continuous monitoring program.

program. Figure 2-8 depicts the Monitor Step with its inputs and outputs along the three organizational tiers.

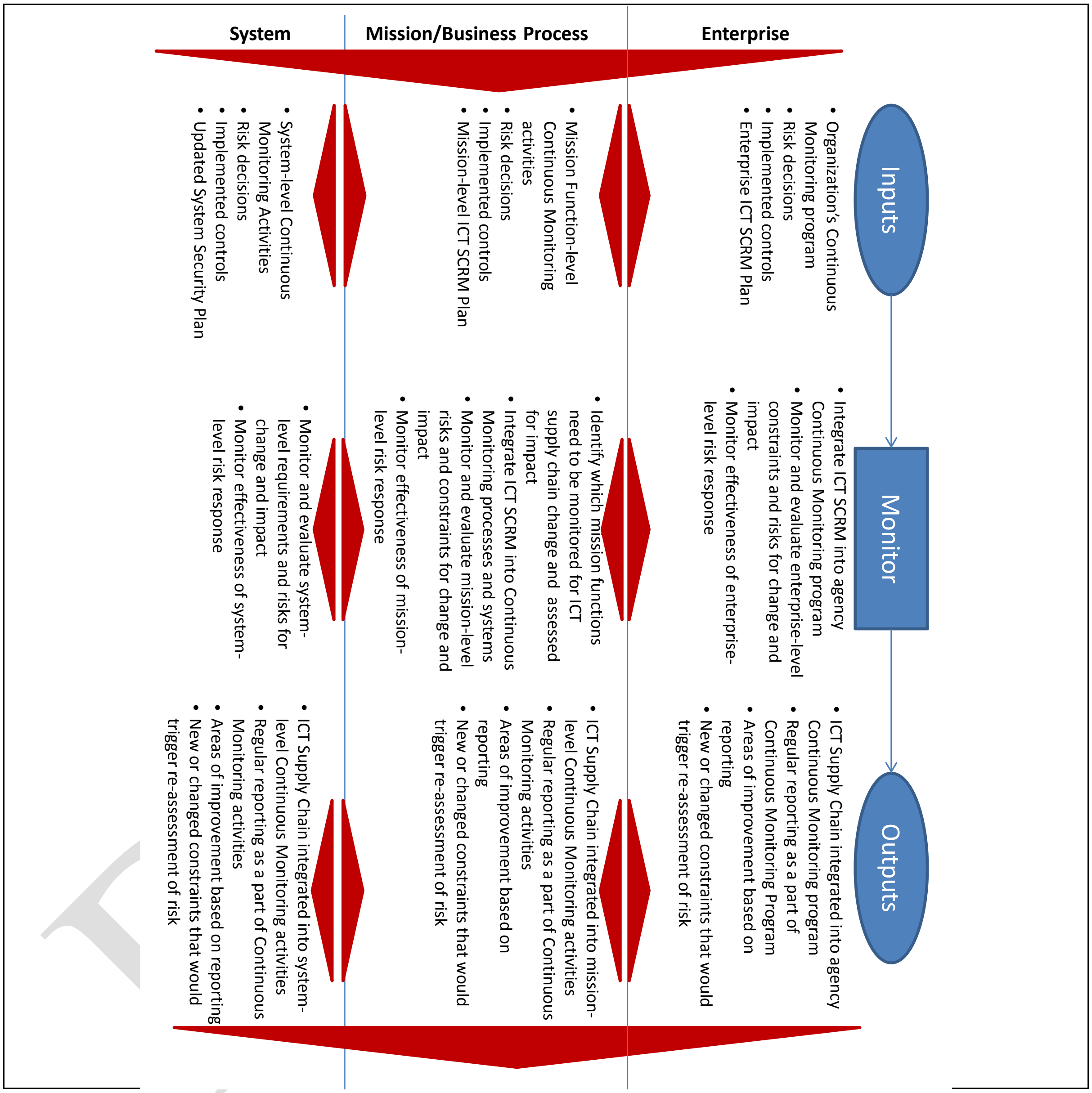

System
Mission/Business Process
Enterprise
Inputs
Organization's Continuous Monitoring program
Risk decisions
Implemented controls
Enterprise ICT SCRM Plan
Mission Function-level Continuous Monitoring activities
Risk decisions
Implemented controls
Mission-level ICT SCRM Plan
System-level Continuous Monitoring Activities
Risk decisions
Implemented controls
Updated System Security Plan
Monitor
Integrate ICT SCRM into agency Continuous Monitoring program
Monitor and evaluate enterprise-level constraints and risks for change and impact
Monitor effectiveness of enterprise-level risk response
Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact
Integrate ICT SCRM into Continuous Monitoring processes and systems
Monitor and evaluate mission-level risks and constraints for change and impact
Monitor effectiveness of mission-level risk response
Monitor and evaluate system-level requirements and risks for change and impact
Monitor effectiveness of system-level risk response
Outputs
ICT Supply Chain integrated into agency Continuous Monitoring program
Regular reporting as a part of Continuous Monitoring Program
Areas of improvement based on reporting
New or changed constraints that would trigger re-assessment of risk
ICT Supply Chain integrated into mission-level Continuous Monitoring activities
Regular reporting as a part of Continuous Monitoring activities
Areas of improvement based on reporting
New or changed constraints that would trigger re-assessment of risk
ICT Supply Chain integrated into system-level Continuous Monitoring activities
Regular reporting as a part of Continuous Monitoring activities
Areas of improvement based on reporting
New or changed constraints that would trigger re-assessment of risk

Figure 2-8. ICT SCRM in the Assess Step

Similarly to Figures 2-4, 2-5, and 2-7, Figure 2-8 depicts inputs, activities, and outputs of the Monitor Step distributed along the three organizational tiers. The large arrows on the left and right sides of the activities depict the inputs from the other steps of the Risk Management Process, with the arrow on the left depicting that the steps are in constant interaction. Inputs into the Monitor Step include inputs from other steps, as well as from the enterprise Continuous Monitoring program and activities. Up-down arrows between the tiers depict flow of information and guidance from the upper tiers to the lower tiers and the flow of information and feedback from the lower tiers to the upper tiers. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

Activities

RISK MONITORING STRATEGY

TASK 4-1: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.

Supplemental Guidance:

Organizations should integrate ICT SCRM considerations into their overall risk monitoring strategy. Because some of the information will be gathered from outside of the agency – from suppliers and integrators, monitoring ICT supply chain risk may require information that agencies have not traditionally collected. The strategy should, among other things, include the data to be collected, the specific measures that will be compiled from the data, identify existing or required tools to collect the data, identify how the data will be protected, and define reporting formats for the data. Potential data sources may include:

- Agency vulnerability management and incident management activities
- Agency manual reviews
- Interagency information sharing
- Information sharing between the agency and system integrator or external service provider
- Supplier information sharing
- Contractual reviews of system integrator or external service provider.

Organizations should ensure appropriate protection of supplier data if that data is collected and stored by the agency. Agencies may also require additional data collection and analysis tools to appropriately evaluate the data to achieve the objective of monitoring applicable ICT supply chain risks.

RISK MONITORING

TASK 4-2: Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

According to NIST SP 800-39, organizations should monitor compliance, effectiveness, and change. Monitoring compliance within the context of ICT SCRM involves monitoring federal agency acquirer processes and ICT products and services for compliance with the established security requirements. Monitoring effectiveness involves monitoring the resulting risk posture to determine whether these established security requirements result in the intended risk posture. Monitoring change involves monitoring the environment for any changes that may result in the change in risk posture and would require changing requirements and mitigations/controls.

To monitor changes, organizations need to identify and document the set of triggers that will result in change in ICT supply chain risk posture. While the categories of triggers will likely include changes to constraints, identified in Table 2-6 (during the Frame Step), including policy, mission, change to the threat environment, enterprise architecture, SDLC, or requirements, the specific triggers within those categories may be substantially different for different organizations.

An example of the ICT supply chain environment change is two key vetted suppliers announcing their departure from a specific market, therefore creating a supply shortage for specific components. This would trigger the need to evaluate whether reducing the number of suppliers would create vulnerabilities in component availability and integrity. In this scenario, potential deficit of components may result simply from insufficient supply of components, which may result from fewer components available. If none of the remaining suppliers are vetted, this deficit may result in uncertain integrity of the remaining components. If the organizational policy directs use of vetted components, this event may result in the organization’s inability to fulfill its mission needs.

In addition to regularly updating existing risks assessments with the results of the ongoing monitoring, the acquirer should determine what would trigger a reassessment. Some of these triggers may include availability of resources, changes to ICT supply chain risk posture, natural disasters, or mission collapse.

Outputs and Post Conditions

Organizations should integrate the ICT supply chain outputs of the Monitor Step into the ICT SCRM Plan. This plan will serve as inputs into iterative implementations of the Frame, Assess, and Respond Steps as required.

CHAPTER THREE

ICT SCRM CONTROLS

During the Respond step of the risk management process, organizations select, tailor, and implement controls for mitigating ICT supply chain risk. Appendix D of NIST 800-53 Rev4 lists a set of information security controls at the FIPS high-, moderate-, and low-impact levels. This chapter uses those controls as a basis for describing controls for high-impact systems which help mitigate risks both to the ICT supply chain itself, and to ICT products and services traversing the ICT supply chain. When needed, specific guidance as to how these controls may be applied to ICT SCRM has been included. NIST defines security controls as:

> *The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.* [19]

NIST SP 800-53 Rev4 defines a number of ICT supply chain controls within the catalog of information security controls. NIST SP 800-161 adds ICT supply chain content to those and some other NIST SP 800-53 Rev4 controls. It also adds Provenance, a new ICT SCRM control family that is not addressed in NIST SP 800-53 Rev4. NIST SP 800-161 refers to all controls that address ICT supply chain, included in NIST SP 800-53 Rev4 and new ones, as ICT SCRM controls.

To create the ICT SCRM-specific control, a variety of existing sources in addition to NIST SP 800-53 Rev4 were examined for relevant information. These additional resources included NISTIR 7622, OTTF, ISO/IEC 27001, ISO/IEC 27002, Draft ISO/IEC 27036, SAFECode Software Integrity documents, DHS Sensitive Systems Policy Directive 4300A, and National Industrial Security Program Operating Manual (NISPOM).

3.1 ICT SCRM CONTROLS OVERLAY

Security controls described in NIST 800-53 Rev4 have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into eighteen families. Each family contains security controls related to the general security topic of the family. A two-character identifier uniquely identifies security control families, for example, PS for Personnel Security. Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices. This chapter is structured as an enhanced overlay of NIST SP 800-53 Rev4 and is therefore organized along the control families in NIST SP 800-53 Rev4 with the addition of the ICT SCRM-specific family, Provenance, therefore creating nineteen control families. Each family provides ICT supply chain guidance that is additional to the already existing content of the family or individual controls contained within the family.

[19] SP 800-53; SP 800-37; SP 800-53A; SP 800-60; FIPS 200; FIPS 199; CNSSI-4009

Additionally, information security controls assessment provided within 800-53A in support of the SP800-53 controls also apply to the SCRM controls in this guidance document.

ICT SCRM is an enterprise activity that requires selection and implementation of controls at the organization, mission, and system levels (Tiers 1, 2, and 3 of the organizational hierarchy according to NIST SP 800-39). Table 3-1 lists control families, including the additional ICT SCRM family, their relevance to ICT SCRM, and the organizational hierarchy tiers in which those controls should be implemented.

Table 3-1. ICT SCRM Control Families

Control Family	Identifier	Tier 1	Tier 2	Tier 3
Access Control	AC	√	√	√
Awareness and Training	AT	√	√	
Audit and Accountability	AU	√	√	√
Security Assessment and Authorization	CA	√	√	√
Configuration Management	CM	√	√	√
Contingency Planning	CP	√	√	
Identification and Authorization	IA	√	√	√
Incident Response	IR	√	√	
Maintenance	MA	√	√	√
Media Protection	MP	√	√	
Physical and Environment Protection	PE	√	√	
Planning Management	PL	√	√	
Personnel Security	PS	√	√	
Provenance	***PV***	√	√	√
Risk Assessment	RA	√	√	
System and Services Acquisition	SA	√	√	√
System and Communications Protection	SC	√	√	√
System and Information integrity	SI	√	√	√
Program Management	PM	√	√	√

3.2 ICT SCRM CONTROLS THROUGHOUT ORGANIZATIONAL HIERARCHY

As noted in Table 3-1, ICT SCRM controls in this document are designated by the three tiers comprising the organizational hierarchy. This is to facilitate ICT SCRM control selection specific to organizations, its various missions, and individual systems, as described in Chapter 2 under Respond Step of the Risk Management Process. During controls selection, organizations should use the ICT SCRM controls in this chapter to identify appropriate ICT SCRM controls for tailoring, per risk assessment. By selecting and implementing applicable ICT SCRM controls for each tier, organizations will ensure that they have appropriately addressed ICT SCRM throughout their enterprises.

3.3 APPLYING ICT SCRM CONTROLS TO ACQUIRING ICT PRODUCTS AND SERVICES

Federal agency acquirers may use ICT SCRM controls to communicate their ICT SCRM requirements to three different types of organizations that provide ICT products and services to federal agencies: system integrators, suppliers, and external service providers. However, the controls in this chapter do not provide specific contracting language. Federal agency acquirers should develop their own contracting language using this document as guidance to develop specific ICT SCRM requirements to be included in contracts.

NIST SP 800-53 Rev4 defines developer as:

> *A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.*

In ICT supply chain, system integrators have a distinct role of assembling information systems, information system components, and information services developed by developers. These components and systems may be developed by other parties also known as vendors or product resellers. NIST SP 800-161 splits the NIST SP 800-53 *developer* into *system integrator* and *supplier*. In this context, *system integrator* refers to item (ii) in the NIST SP 800-53 Rev4 definition while *Supplier* refers to items (i), (iii), and (iv).

3.3.1 System Integrators

System integrators are those organizations that provide customized services to the federal agency acquirer including custom development, test, and operations and maintenance. This group usually replies to a request for proposal from a federal agency acquirer with a proposal that describes solution or services that are customized to the federal agency acquirer requirements. Such proposals provided by system integrators can include many layers of suppliers (see 3.3.2). The system integrator should carry the responsibility for ensuring that those suppliers are vetted and verified with the respect to federal agency acquirer ICT SCRM requirements. Because of the level of visibility that can be obtained in the relationship with the system integrator, the federal agency acquirer has the ability to require a rigorous supplier acceptance criteria as well as any relevant countermeasures to address identified or potential risks.

3.3.2 Suppliers

Suppliers are those organizations providing either commercial off-the-shelf (COTS) or government off-the-shelf solutions to the federal agency acquirer. COTS include non-developmental items (NDI) such as commercially licensing solutions/products as well as Open Source Solutions (OSS). Government off-the-shelf (GOTS) are government-only license-able solutions. Suppliers are a very diverse group, ranging from small to large, based in a single country to transnational, and range widely in the level of sophistication, resources, and transparency/visibility in both process and solution. Suppliers also have rather diverse levels of foundational practices and ICT SCRM practices.

The organizations should consider that supplier costs of doing business are directly proportional to the level of visibility into how they apply security controls to their solutions. This means that when organizations or system integrators require greater levels of transparency from suppliers, they have to consider cost implications of such requirements.   Suppliers may select to not participate in procurements to avoid increased costs and therefore limit organizations' technology choices. The risk to suppliers is that of multiple different sets of requirements that they have to individually comply with, which is not scalable. However, numerous efforts are under way to provide for ICT SCRM baselines, in addition to this document, that aim to help manage this risk.

3.3.2 External Providers of Information System Services

Organizations continue to expand their use of external providers' IT services to manage their mission and business functions.[20] Federal agency acquirer outsourcing of IT services or the hosting of IT infrastructure or services to an external provider creates a set of ICT supply chain concerns that reduces federal agency acquirer visibility into, and control of, the outsourced functions. It therefore requires increased rigor from the organizations in defining ICT SCRM requirements, stating them in procurements, and then monitoring delivered services and evaluating them for compliance with these requirements. Regardless of who performs the services, the federal agency acquirer is ultimately responsible and accountable for the risk to the federal agency systems and information that may result from using these services. This means that organizations should implement a set of compensating ICT SCRM controls to address this risk and work with the federal agency risk executive to accept this risk. A variety of methods may be used to communicate and subsequently verify and monitor ICT SCRM requirements through such vehicles as contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain transactions. These methods include:

- Clearly defining the types of external services provided to the external organization;
- Describing how the external services should be protected in accordance with the federal agency ICT supply chain security requirements; and
- Obtaining the necessary verifications that the risk to the organizations' organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable.

3.4 SELECTING, TAILORING, AND IMPLEMENTING ICT SCRM SECURITY CONTROLS

Once the federal agency selects ICT SCRM controls from the set defined in this chapter, these controls should be tailored to the individual federal agency's needs and environment to ensure a cost-effective, risk-based approach to providing ICT SCRM enterprise-wide using the tailoring guidance in NIST SP 800-53 Rev4. The tailoring should be coordinated with and approved by appropriate organizational officials (e.g., authorizing officials, authorizing official designated representatives, risk executive (function), chief information officers, or senior information security officers) prior to implementing the ICT SCRM controls. Additionally, federal agencies should perform the tailoring process at the organization level (either as the required tailored baseline or as the starting point for policy, program or system-specific tailoring), at the program, individual information system level, or using a combination of organization-level, program/mission-level and system-specific approaches. Tailoring decisions for all affected ICT SCRM controls, including the specific rationale for those decisions, should be documented in the ICT SCRM Plans for Tiers 1, 2, and 3 and approved by appropriate organizational officials as part of the ICT SCRM Plan approval process. After selecting the initial set of security controls from Chapter 3, the federal agency acquirer should initiate the tailoring process according to the NIST SP 800-53 Rev4 to appropriately modify and more closely align the controls with the specific conditions within the organization.

[20] NIST SP800-53rev 4, Section 2.4, Security Controls in External Environments, page 12.

Organizations should document the resulting tailored ICT SCRM controls in the ICT SCRM Plan, following guidance from NIST SP 800-53 Rev4.

3.4.1 ICT SCRM Control Format

Table 3-2 shows the format used in this document for controls which provide supplemental ICT SCRM guidance on existing NIST SP 800-53 Rev. 4 controls or control enhancements. Each control is hyperlinked to the appropriate parent control in Appendix D. ICT SCRM controls that do not have a parent NIST SP 800-53 Rev. 4 control follow the format described in NIST SP 800-53 Rev. 4.

Table 3-2. ICT SCRM Control Format

SCRM CONTROL IDENTIFIER	**CONTROL NAME**	**PARENT NIST SP 800-53 CONTROL**
	Supplemental ICT SCRM Guidance:	
	TIERS:	
	Control Enhancements:	
(#)	***CONTROL NAME | CONTROL ENHANCEMENT NAME***	**PARENT NIST SP 800-53 CONTROL ENHANCEMENT**
	Supplemental ICT SCRM Guidance:	
	TIERS:	

An example of the ICT SCRM control format is AC-3 and AC-3(1):

SCRM_AC-3 **ACCESS ENFORCEMENT** **AC-3**

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

Control Enhancements:

(1) *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS* *AC-3 (8)*

Supplemental ICT SCRM Guidance: Prompt revocation is critical for ICT supply chain security to ensure that system integrators, suppliers, and external service providers who no longer require access are not able to access federal agency acquirer system. For example, in a “badge flipping” situation, a contract is transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the federal agency acquirer should retire the old credentials and issue completely new credentials.

TIER: 2, 3

3.4.2 Using ICT SCRM Controls in This Document

The remainder of Chapter 3 will provide the enhanced ICT SCRM overlay of NIST SP 800-53 Rev4. Appendix D will provide the description of NIST SP 800-53 Rev4 controls, the enhancements for which are included in Section 3. Specifically, Chapter 3 will display the relationship between NIST SP 800-53 Rev4 controls and ICT SCRM controls in one of the following ways:

- If a NIST SP 800-53 Rev4 control or enhancement was determined to be a purely information security control that serves as a foundational control for ICT SCRM but is not specific to ICT SCRM, it is not included in this document.
- If a NIST SP 800-53 Rev4 control or enhancement was determined to be relevant to ICT SCRM, only the title of that control or enhancement is included in Chapter 3 with the complete control provided in Appendix D.
- If a NIST SP 800-53 Rev4 control was enhanced by ICT SCRM content, only additional text is included in Chapter 3 with the complete control (unchanged from NIST SP 800-53 Rev4) provided in Appendix D.
- The new control family, Provenance, is included in Chapter 3 in its entirety.

3.5 ICT SCRM SECURITY CONTROLS

FAMILY: ACCESS CONTROL

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

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

Systems and components that traverse the ICT supply chain and infrastructure are subject to access by a variety of individuals within federal agency acquirer, system integrator, supplier, or external service provider organizations. Such access should be defined and managed to ensure that it does not inadvertently result in unauthorized release, modification, or destruction of sensitive federal agency information or sensitive system integrator, supplier, and external service provider information. This access should be limited to only the necessary access for authorized individuals and monitored for ICT supply chain impact.

SCRM_AC-1 ACCESS CONTROL POLICY AND PROCEDURES AC-1

Supplemental ICT SCRM Guidance: Organizations should specify and include in agreements (e.g., contracting language) access control policies for their system integrators, suppliers, and external service providers. These should include both physical and logical access.

TIER: 1, 2, 3

SCRM_AC-2 ACCOUNT MANAGEMENT AC-2

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_AC-3 ACCESS ENFORCEMENT

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

Control Enhancements:

(2) *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS* *AC-3 (8)*

Supplemental ICT SCRM Guidance: Prompt revocation is critical for ICT supply chain security to ensure that system integrators, suppliers, and external service providers who no longer require access are not able to access a federal agency acquirer system. For example, in a “badge flipping” situation, a contract is transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the federal agency acquirer should retire the old credentials and issue completely new credentials.

TIER: 2, 3

SCRM_AC-4 INFORMATION FLOW ENFORCEMENT AC-4

Control Enhancements:

(1) *INFORMATION FLOW ENFORCEMENT | METADATA* *AC-4 (6)*

Supplemental ICT SCRM Guidance: In ICT SCRM, information about systems and system components, acquisition details, and delivery is considered metadata and should be appropriately protected. Metadata relevant to ICT SCRM is quite extensive and includes activities within the SDLC. Organizations should identify which metadata is directly relevant to their ICT supply chain security.

TIER: 2, 3

(2) *INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION* *AC-4 (17)*

Supplemental ICT SCRM Guidance: Within ICT SCRM context, organizations should specify various source and destination points for information about ICT supply chain and information that flows through the supply chain. This is so that organizations have visibility into the physical and logical origins of systems and components that they use.

TIER: 2, 3

(3) *INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA* *AC-4 (19)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(4) *INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS* *AC-4 (21)*

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_AC-5 SEPERATION OF DUTIES **AC-5**

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_AC-6 LEAST PRIVILEGE **AC-6**

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_AC-7 REMOTE ACCESS **AC-17**

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

Control Enhancements:

(1) *REMOTE ACCESS | PROTECTION OF INFORMATION* *AC-17 (6)*

TIER: 2, 3

SCRM_AC-8 WIRELESS ACCESS **AC-18**

Supplemental ICT SCRM Guidance: Federal agency acquirer's wireless infrastructure may include supply chain logistics infrastructure such as Radio Frequency Identification Devices (RFID), tracking sensors during shipping, and other similar technologies. Acquirers should explicitly define appropriate wireless access control mechanisms for supply chain and logistics infrastructure in policy and implement those mechanisms.

TIER: 1, 2, 3

SCRM_AC-9 ACCESS CONTROL FOR MOBILE DEVICES AC-19

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_AC-10 USE OF EXTERNAL INFORMATION SYSTEMS AC-20

Supplemental ICT SCRM Guidance: Organizations' external information systems include those of system integrators, suppliers, and external service providers. Unlike in federal agency acquirer's internal organizations where direct and continuous monitoring is possible, in the external supplier relationship, information is shared on an as-needed basis and should be articulated in an agreement. Access from such external information systems should be monitored and audited.

TIER: 1, 2, 3

Control Enhancements:

(1) *USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE* *AC-20 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES* *AC-20 (3)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_AC-11 COLLABORATION AND INFORMATION SHARING AC-21

Supplemental ICT SCRM Guidance: Sharing information within the ICT supply chain helps to manage ICT supply chain risks. This information may include vulnerabilities, threats, criticality of systems and components, or delivery information. However, this information sharing should be carefully managed to ensure that the information is accessible only to authorized individuals within the ICT supply chain. Organizations should clearly define boundaries for information sharing, such as temporal, informational, contractual, security, access, system and others. Organizations should monitor and review for unintentional or intentional of information sharing within its ITC supply chain activities including information sharing with system integrators, suppliers, and external service providers.

TIER: 1, 2

SCRM_AC-12 PUBLICLY ACCESSIBLE CONTENT AC-22

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

TIER: 2, 3

SCRM_AC-13 ACCESS CONTROL DECISIONS AC-24

Supplemental ICT SCRM Guidance: Organizations should include ICT SCRM requirements in access control decisions for supply chain systems, processes, or roles across the SDLC.

TIER: 1, 2, 3

FAMILY: AWARENESS AND TRAINING

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

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

NIST SP 800-161 expands the Awareness and Training control of FIPS 200 to include ICT SCRM. Making workforce aware of ICT SCRM concerns is key to a successful ICT SCRM strategy. ICT SCRM awareness and training provides understanding of the problem space and of the appropriate processes and controls that can help mitigate ICT supply chain risk. Federal agencies should provide ICT SCRM awareness and training to individuals at all levels within the organization including, for example, risk executive function, acquisition and contracting professionals, program managers, supply chain and logistics professionals, shipping and receiving staff, information technology professionals, quality professionals, mission and business owners, system owners, and information security engineers. Organizations should also work with system integrators and external service providers to ensure that their personnel that interact with federal agency ICT supply chains receive appropriate ICT SCRM awareness and training, as appropriate.

SCRM_AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES AT-1

Supplemental ICT SCRM Guidance: Organizations should integrate ICT supply chain risk management training and awareness policy into the security training and awareness policy. The ICT SCRM training should target both the acquirer and its system integrators. The policy should ensure that ICT supply chain role-based training is required for those individuals who touch or impact the ICT supply chain and its security, such as system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response.

ICT SCRM training procedures should address:

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

TIER: 1, 2

SCRM_AT-2 SECURITY TRAINING AT-3

Control Enhancements:

(1) *SECURITY TRAINING | PHYSICAL SECURITY CONTROLS* AT-3 (2)

Supplemental ICT SCRM Guidance: ICT SCRM is impacted by a number of physical security mechanisms and procedures for both the supply chain systems and the systems traversing the supply chain, such as manufacturing, shipping and receiving, physical access to facilities, inventory management, and warehousing. Acquirer and system integrator personnel providing development and operational support to the acquirer should receive training on how to handle these physical security mechanisms and on the associated ICT supply chain risks.

TIER: 2

FAMILY: AUDIT AND ACCOUNTABILITY

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

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

Audit and accountability are important for ICT supply chain to provide information about what happened in the federal agency supply chain in case of an ICT supply chain compromise. Organizations should ensure that they designate ICT supply chain-relevant events and audit for those events within their own system boundaries using appropriate audit mechanisms (e.g., system logs, IDS logs, firewall logs). Organizations may encourage their system integrators and external service providers to do the same and may include contract clauses that require such monitoring. However, organizations should not deploy audit mechanisms on the systems outside of their agency boundary including those of system integrators and external service providers.

SCRM_AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES AU-1

Supplemental ICT SCRM Guidance: Audit mechanisms provide data for tracking activities in federal agency acquirer ICT supply chain infrastructure. Audit and accountability policy and procedures should appropriately address such tracking and its availability for other federal agency acquirer ICT supply chain activities, such as configuration management. System integrator, supplier, and external service provider activities should not be included in such policy, unless those are performed on federal agency acquirer's information systems.

TIER: 1, 2, 3

SCRM_AU-2 AUDITABLE EVENTS AU-2

Supplemental ICT SCRM Guidance: An ICT supply chain auditable event is an observable occurrence within the supply chain infrastructure or the system traversing the supply chain. Such events should be identified as ICT supply chain auditable events and captured by appropriate audit mechanisms. ICT supply chain events should be identified as auditable based on federal agency acquirer SDLC context. For example, include tracking change and handoff of software source code to ensure that it is authorized, traceable, and verifiable.

TIER: 1, 2, 3

SCRM_AU-3 CONTENT OF AUDIT RECORDS AU-3

TIER: 2, 3

SCRM_AU-4 AUDIT REVIEW, ANALYSIS, AND REPORTING AU-6

Supplemental ICT SCRM Guidance: For ICT SCRM, the federal agency acquirer should ensure that both ICT supply chain and information security events are appropriately filtered and correlated for analysis and reporting. For example, if new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of the patch arrival qualifies as ICT supply chain auditable event, while invalid signature is an information security auditable event. The combination of these two events indicates an ICT supply chain auditable event.

TIER: 2,3

Control Enhancements:

(1) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING* *AU-6 (6)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INPUT FROM NON-TECHNICAL SOURCES* *AU-6 (9)*

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

TIER: 3

SCRM_AU-5 NON-REPUDIATION

Control Enhancements:

(1) *NON-REPUDIATION | ASSOCIATION OF IDENTITIES* *AU-10 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 2

(2) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODCUER IDENTITIY* *AU-10 (2)*

Supplemental ICT SCRM Guidance: None

TIER: 2,3

(3) *NON-REPUDIATION | CHAIN OF CUSTODY* *AU-10 (3)*

Supplemental ICT SCRM Guidance: None

TIER: 2,3

(4) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY* *AU-10 (4)*

Supplemental ICT SCRM Guidance: None

TIER: 2,3

SCRM_AU-6 MONITORING FOR INFORMATION DISCLOSURE **AU-13**

Supplemental ICT SCRM Guidance: Within ICT SCRM context, information disclosure may occur via multiple avenues including open source information. For example, supplier-provided errata may reveal information about a federal agency acquirer system that may provide insight into the system that increases the risk to the system.

TIER: 2,3

SCRM_AU-7 CROSS-ORGANIZATIONAL AUDITING AU-16

Supplemental ICT SCRM Guidance: In ICT SCRM context, this control includes organizations' use of system integrator or external service provider organizational infrastructure.

TIER: 2,3

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

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

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

Organizations should integrate ICT supply chain considerations, including risks and controls, into ongoing security assessment and authorization activities. This includes activities to assess and authorize internal agency systems, as well as external assessments of system integrators and external service providers, where appropriate. ICT supply chain aspects include documentation and tracking of chain of custody and system interconnections within and between organizations, verification of ICT supply chain security training, verification of suppliers claims of conformance to security, product/component integrity, and validation tools and techniques for noninvasive approaches to detect counterfeits or malware (e.g., Trojans) using inspection for genuine components including manual inspection techniques.

SCRM_CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES *CA-1*

Supplemental ICT SCRM Guidance: Integrate the development and implementation of assessment and authorization policies and procedures for ICT supply chain security into the security assessment and authorization policy. ICT supply chain aspects include documentation and tracking of chain of custody and system interconnections within and between organizations, verification of ICT supply chain security training, verification of suppliers claims of conformance to security, product/component integrity, and validation tools and techniques for noninvasive approaches to detect counterfeits or malware (e.g., Trojans) using inspection for genuine components including manual inspection techniques.

TIER: 1, 2, 3

SCRM_CA-2 SECURITY ASSESSMENTS *CA-2*

Supplemental ICT SCRM Guidance: Ensure that the security assessment plan incorporates SCRM requirements on an individual system-by-system basis.

TIER: 3

Control Enhancements:

(1) *SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS* *CA-2 (2)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS* CA-2 (3)

Supplemental ICT SCRM Guidance: For ICT SCRM, organizations may use external assessments for system integrators, suppliers, and external service providers. External assessments include certifications and third- party assessments, such as those driven by organizations such as the International Organization for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and The Open Group Trusted Technology Forum (TTF) if such certifications meet agency needs.

TIER: 3

SCRM_CA-3 SYSTEM INTERCONNECTIONS CA-3

Supplemental ICT SCRM Guidance: Interconnected systems and mission operations require scrutiny from a supply chain perspective. This includes understanding whether those components/systems that are directly interconnected with system integrators, external service providers and, in some cases, suppliers. Examples of such connections can include:

a. A shared development and operational environment between acquirer and system integrator;
b. Product update/patch management connection to an Off-The-Shelf (OTS) supplier; and
c. Data request and retrieval transactions into processing system residing on an external service provider shared environment.

TIER: 3

Control Enhancements:

(1) *INFORMATION SYSTEM CONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS* CA-3 (3)

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS* CA-3 (4)

Supplemental ICT SCRM Guidance: For ICT SCRM, ensure that the system integrator and external service provider appropriately protect connections to public networks. Implement appropriate processes for review and inspection, evidence gathering, and incident management.

Supplemental ICT SCRM Guidance: None

TIER: 3

(3) *SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS* CA-3 (5)

Supplemental ICT SCRM Guidance: For ICT SCRM, ensure that the system integrator and external service provider appropriately protect connections to public networks. Implement appropriate processes for review and inspection, evidence gathering, and incident management.

TIER: 3

SCRM_CA-4 PLAN OF ACTION AND MILESTONES CA-5

TIER: 2, 3

SCRM_CA-5 SECURITY AUTHORIZATIONS *CA-6*

Supplemental ICT SCRM Guidance: Authorizing officials should include ICT supply chain considerations in authorization decisions. To accomplish this, ICT supply chain risks and compensating controls documented in ICT SCRM Plans or system security plans should be included in the decision-making process.

TIER: 1, 2, 3

SCRM_CA-6 CONTINUOUS MONITORING

Supplemental ICT SCRM Guidance: In addition to NIST SP 800-53 Revision 4 control description, see Chapter 2 for more information.

TIER: 1, 2, 3

Control Enhancements:

(1) *CONTINUOUS MONITORING | TREND ANALYSES* CA-7(3)

Supplemental ICT SCRM Guidance: Information gathered during continuous monitoring serves as inputs into ICT SCRM decisions including criticality analysis, vulnerability and threat analysis, and risk assessment. It also provides information that can be used in incident response and potentially identify ICT supply chain compromise.

TIER: 3

FAMILY: CONFIGURATION MANAGEMENT

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

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

Configuration Management helps track systems, components, and documentation throughout the ICT supply chain. This is important for knowing what changes were made to those systems, components, and documentation, who made the changes, and who authorized the changes. Basically, configuration management provides the tools to establish the chain of custody for systems, components, and documentation. Configuration management also provides evidence for ICT supply chain compromise investigations when determining which changes were authorized and which were not, which can provide useful information. Organizations should apply configuration management controls to their own systems and encourage use of configuration management controls by their system integrators, suppliers, and external service providers.

SCRM_CM-1 CONFIGURATION MANGEMENT POLICY AND PROCEDURES CM-1

Supplemental ICT SCRM Guidance: Configuration management is a critical activity that impacts nearly every aspect of ICT supply chain security. When defining configuration management policy and procedures, organizations should address the full SDLC. This should include procedures for introducing and removing components to and from the agency as configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata.

TIER: 1, 2, 3

SCRM_CM-2 BASELINE CONFIGURATION CM-2

Supplemental ICT SCRM Guidance: Organizations should establish a baseline configuration of both ICT supply chain systems and those systems traversing the ICT supply chain by documenting, formally reviewing, and agreed to by stakeholders. The baseline configuration must take into consideration acquirer and any relevant system integrator, supplier , and external service provider involvement within the acquirer infrastructure where relevant. If the system integrator, for example, uses the existing ederal agency acquirer’s infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation.

TIER: 2,3

Control Enhancements:

(1) *BASELINE CONFIGURATION | REVIEWS AND UPDATES* CM-2 (1)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *ACCESS RESTRICTIONS FOR CHANGE | DEVELOPMENT AND TEST ENVIRONMENTS* CM-2 (6)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_CM-3 CONFIGURATION CHANGE CONTROL CM-3

Supplemental ICT SCRM Guidance: Organizations should determine, implement, and monitor configuration change controls for federal agency ICT supply chain systems. This control supports traceability for ICT SCRM.

Control Enhancements:

(1) *CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES* CM-3 (1)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES* CM-3 (2)

Supplemental ICT SCRM Guidance: None

TIER: 2,3

SCRM_CM-4 SECURITY IMPACT ANALYSIS CM-4

Supplemental ICT SCRM Guidance: Federal agency acquirer should evaluate changes to the ICT supply chain systems and the systems traversing the ICT supply chain to determine whether the impact of these changes warrants additional protection to maintain an acceptable level of ICT supply chain risk.

TIER: 3

Control Enhancements:

(1) *SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS* CM-4(1)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_CM-5 ACCESS RESTRICTIONS FOR CHANGE CM-5

TIER: 2, 3

Control Enhancements:

(1) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING* CM-5(1)

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES* CM-5(2)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS* CM-5(3)

Supplemental ICT SCRM Guidance: This control addresses tamper resistance and aids in verifying that the software is valid, unchanged, and originated from the expected source.

TIER: 3

(4) *ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES* CM-5(6)

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

TIER: 3

SCRM_CM-6 CONFIGURATION SETTINGS CM-6

Supplemental ICT SCRM Guidance: Federal agency acquirer should oversee the function of modifying configuration settings if performed by system integrator or external service provider to ensure compliance with policy. Methods of oversight include periodic verification, reporting, and review. This information may be shared with various parties within the ICT supply chain infrastructure on a need-to-know basis.

TIER: 2, 3

Control Enhancements:

(1) *CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION* CM-6(1)

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES* CM-6(2)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_CM-7 LEAST FUNCTIONALITY CM-7

Supplemental ICT SCRM Guidance: Within ICT SCRM context, least functionality reduces the attack surface. Organizations should select components that allow the flexibility and options for specifying and implementing least functionality.

TIER: 3

Control Enhancements:

(1) *LEAST FUNCTIONALITY | PERIODIC REVIEW* CM-7(1)

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE/BLACKLISTING* CM-7(4)

Supplemental ICT SCRM Guidance: Organizations may define requirements and deploy appropriate processes to specify allowable and not allowable software. This should include requirements for alerts when software is introduced into the federal agency acquirer environment. An example is to allow only open source software if its code is available for federal agency acquirer evaluation.

TIER: 2, 3

(3) *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE/WHITELISTING* CM-7(5)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_CM-8 INFORMATION SYSTEM COMPONENT INVENTORY CM-8

TIER: 2, 3

Control Enhancements:

(1) *INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS* *CM-8(1)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE* *CM-8(2)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(3) *INFORMATION SYSTEM COMPONENT INVENTORY | PROPERTY ACCOUNTABILITY INFORMATION* *CM-8(4)*

Supplemental ICT SCRM Guidance: Organizations should ensure that individuals who originated the acquisition and intended end users are identified in the property accountability information.

TIER: 3

(4) *INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS* *CM-8(6)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(5) *INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY* *CM-8(7)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(3) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING* *CM-8(8)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(6) *INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS* *CM-8(9)*

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_CM-9 CONFIGURATION MANAGEMENT PLAN CM-9

Supplemental ICT SCRM Guidance: Organizations should ensure that ICT SCRM considerations are incorporated into the configuration management planning activities.

TIER: 2, 3.

Control Enhancements:

(1) *CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY* *CM-9(1)*

Supplemental ICT SCRM Guidance: Federal Agency acquirer should ensure that all relevant roles are defined to address configuration management activities for ICT supply chain systems and those systems traversing the ICT supply chain. Federal Agencies should ensure that the following ICT supply chain activities are appropriately included in the configuration management plan: development, sustainment, test, market analysis, RFP development and review/approval, procurement, integration, sustainment, and maintenance.

TIER: 2, 3

SCRM_CM-10 SOFTWARE USAGE RESTRICTIONS CM-10

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

Control Enhancements:

(2) *SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE* *CM-10(1)*

Supplemental ICT SCRM Guidance: When considering software, organizations should review all options and corresponding risks including commercially licensed and open source components. As an alternative to commercially licensed software, use of open source software requires an understanding of provenance, configuration management, source availability for testing and use, and much more. Numerous open source solutions are currently in use by federal agencies, such as those that provide integrated development environments (IDE) and web servers.

TIER: 2, 3

SCRM_CM-11 USER-INSTALLED SOFTWARE CM-11

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

FAMILY: CONTINGENCY PLANNING

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

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

ICT supply chain concerns of contingency planning include planning for alternative suppliers of system components, alternative suppliers of systems and services, and planning for alternate delivery routes for critical system components. Additionally, many techniques used for contingency planning, such as alternative processing sites, have their own ICT supply chains including their own specific ICT supply chain risks. Federal agencies should ensure that they understand and manage ICT supply chain risks and dependencies related to the contingency planning activities as necessary.

SCRM_CP-1 CONTIGENCY PLANNING POLICY AND PROCEDURES CP-1

Supplemental ICT SCRM Guidance: Organizations should integrate ICT supply chain concerns into the contingency planning policy. The policy should cover ICT supply chain systems and the systems traversing the supply chain and address:

a. Unplanned components failure and subsequent replacement;
b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and
c. Product unavailability.

TIER: 1, 2, 3

SCRM_CP-2 CONTIGENCY PLAN CP-2

Supplemental ICT SCRM Guidance: None.

TIER: 3

Control Enhancements:

(1) *CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS* *CP-2 (7)*

Supplemental ICT SCRM Guidance: None.

TIER: 3

(2) *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS* *CP-2 (8)*

Supplemental ICT SCRM Guidance: This control and enhancement supports criticality analysis at the information system level.

TIER: 3

SCRM_CP-3 ALTERNATE STORAGE SITE CP-6

Supplemental ICT SCRM Guidance: When managed by system integrators or external service providers, alternate storage sites are considered within federal agency acquirer ICT supply chain infrastructure. In that case, organizations should apply appropriate ICT supply chain controls.

TIER: 2, 3

SCRM_CP-4 ALTERNATE PROCESSING SITE CP-7

Supplemental ICT SCRM Guidance: When managed by system integrators or external service providers, alternate processing sites are considered within federal agency acquirer ICT supply chain infrastructure. In that case, organizations should apply appropriate ICT supply chain controls.

TIER: 2, 3

SCRM_CP-5 TELECOMMUNICATIONS SERVICES CP-8

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

Control Enhancements:

(1) *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS* *CP-8 (3)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(2) *TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN* *CP-8 (4)*

Supplemental ICT SCRM Guidance: For ICT SCRM, system integrator and external service provider contingency plans should provide separation in infrastructure, service, process, and personnel where appropriate.

TIER: 2, 3

FAMILY: IDENTIFICATION AND AUTHENTICATION

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

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

NIST SP 800-161 expands the FIPS 200 identification and authentication control family to include identification and authentication of components, in addition to individuals (users) and processes acting on behalf of individuals. Identification and authentication is critical for ICT SCRM because it provides traceability of individuals, processes acting on behalf of individuals, and specific systems/components in federal agency acquirer ICT supply chains. Identification and authentication is required to appropriately manage ICT supply chain risks to both reduce risks of ICT supply chain compromise and to help have needed evidence in case of ICT supply chain compromise.

SCRM_IA-1 IDENTIFICATION AND AUTHENCITCATION POLICY AND PROCEDURES IA-1

Supplemental ICT SCRM Guidance: Organizations should enhance their identity and access management policies for ICT SCRM to ensure that critical acquirer roles are defined and critical acquirer systems, components, and processes are identified for traceability. It is important not to provide identity for all things in the ICT supply chain that are cost-prohibitive and too voluminous to process. This should include the identity of components that in the past were not considered under identification and authentication.

TIER: 1,2,3

SCRM_IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) IA-2

Supplemental ICT SCRM Guidance: None.

TIER: 1,2,3

SCRM_IA-3 IDENTIFIER MANAGEMENT IA-4

Supplemental ICT SCRM Guidance: Especially in the ICT SCRM context, identifiers are not limited to those for individuals; identifiers also should be assigned to documentation, devices, and components throughout the agency SDLC, from concept to retirement. The benefit of having these identifiers is greater visibility within organizations ICT supply chain infrastructure.

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

System integrators, suppliers, and external service providers typically use their own identifiers for tracking within their own ICT supply chain infrastructures. Federal agencies should correlate those identifiers with the agency-assigned identifiers for traceability and accountability.

TIER: 2,3

Control Enhancements:

(1) *IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS* IA-4 (4)

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(2) *IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT* IA-4 (5)

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(3) *IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT* IA-4 (6)

Supplemental ICT SCRM Guidance: None.

TIER: 1, 2, 3

SCRM_IA-4 AUTHENTICATOR MANAGEMENT IA-5

Supplemental ICT SCRM Guidance: None.

TIER: 2,3

Control Enhancements:

(1) *AUTHENTICATOR MANAGEMENT | CHANGE AUTHEITICATORS PRIOR TO DELIVERY* IA-5 (5)

Supplemental ICT SCRM Guidance: None.

TIER: 3

(2) *AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANGEMENT* IA-5 (9)

Supplemental ICT SCRM Guidance: None.

TIER: 3

SCRM_IA-5 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) IA-8

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

FAMILY: INCIDENT RESPONSE

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

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

ICT supply chain compromises may span federal agency, system integrators, suppliers, and external service provider systems and organizations. Organizations should ensure that their incident response controls address ICT supply chain concerns including how information about incidents will be shared with system integrators, suppliers, and external service integrators. Incident response will help determine whether an incident is related to the ICT supply chain.

SCRM_IR-1 IDENTIFICATION AND AUTHENCITCATION POLICY AND PROCEDURES IR-1

Supplemental ICT SCRM Guidance: Integrate ICT SCRM considerations into incident response policy and procedures. ICT supply chain-related incidents and those cybersecurity incidents that may complicate or impact ICT supply chain concerns must be defined in the policy. Additionally, the policy should define when, how, and with whom to communicate within the broader ICT supply chain security stakeholders and ICT supply chain partners in the event of an incident. This communication should be defined in agreements with system integrators, suppliers, and external service providers and be bidirectional to inform all involved parties. Depending on the severity of the incident, the need to accelerate communications upstream and downstream may be necessary. Appropriate agreements should be put in place with system integrators, suppliers, and external service providers to ensure speed of communication, response, corrective actions, and other related activities.

Individuals working within specific mission and system environments need to recognize and report ICT supply chain-related incidents. Policy should state when and how this reporting is to be done. Additionally, communications response process must be defined addressing when, how, and with whom to communicate with the broader supply chain security stakeholders and supply chain partners in the event of an incident.

Additionally, in Tiers 2 and 3, procedures and organization-specific incident response methods must be in place, training completed, and coordinated communication established among acquirer and its many suppliers to ensure efficient coordinated incident response effort.

TIER: 1, 2, 3

SCRM_IR-2 INCIDENT HANDELING

Control Enhancements:

(1) *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION* IR-4 (10)

Supplemental ICT SCRM Guidance: In many cases, a number of organizations are involved in managing incidents and responses for supply chain security. Acquirers and their system integrators, suppliers, and external service providers need to conduct coordinated communications, incident response, root cause, and corrective actions activities. Securely sharing information through a coordinated set of personnel in key roles will allow for a more comprehensive approach which is key for handling incidents. Acquirers need to work closely with system integrators, suppliers, and external service providers for the handling of incidents. Therefore, selecting system integrators, suppliers, and external service providers with mature capabilities for supporting incident handling is important for handling ICT SCRM incidents. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A review (and potential revision) of the agreement is recommended, based on the lessons learned from previous incidents.

TIER: 2

SCRM_IR-3 INCIDENT REPORTING **IR-6**

TIER: 3

Control Enhancements:

(1) *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION* IR-6 (3)

Supplemental ICT SCRM Guidance: The reporting of security incident information from the acquirer to the supplier or from the supplier to the acquirer requires protection. Measures must be taken to ensure that the information is reviewed and approved for sending based on acquirer/supplier agreements. The methods of communications regarding such data must ensure that the data is adequately protected for transmission and received by approved individuals within the organization only.

TIER: 3

SCRM_IR-4 INFORMATION SPILLAGE RESPONSE **IR-9**

Supplemental ICT SCRM Guidance: The ICT supply chain is vulnerable to information spillage. Therefore, information spillage response activities should include ICT supply chain-related information spills. This may require coordination with system integrators, suppliers, and external service providers. The details of how this coordination is to be conducted should be included in the agreement (e.g., contract). See SA-4.

TIER: 3

FAMILY: MAINTENANCE

FIPS 200 specifies the Maintenance minimum security requirement as follows:

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

Maintenance is frequently performed by an organization that is different from the federal agency. As such, maintenance becomes part of the ICT supply chain. Maintenance includes performing updates and replacements. The entire SP 800-161 can be applied to a maintenance situation including assessing the ICT supply chain risks, selecting ICT SCRM controls, implementing these controls, and monitoring them.

SCRM_MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES MA-1

Supplemental ICT SCRM Guidance: Organizations should ensure that ICT supply chain concerns are included in maintenance policies and procedures for all organizational information systems. With standard maintenance contracts, mission, organization and system-specific objectives and requirements are shared between agency and system integrator leaving room for significant vulnerabilities and insider opportunities for attack. In many cases, the maintenance of systems is outsourced to a system integrator and as such, appropriate measures must be taken to ensure proper assessment of the organization and its IT infrastructure doing maintenance. Even when maintenance is not outsourced, the upgrades and patches, frequency of maintenance, replacement parts, and other aspects of system maintenance are affected by the supply chain.

Maintenance policies should be defined both for the systems traversing the supply chain and the agency supply chain infrastructure. The maintenance policy should reflect appropriate controls based on an applicable risk assessment within the maintenance context, such as remote access, roles and attributes of maintenance personnel that have access, the frequency of updates, duration of contract, logistical path used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, source code, test cases, and other item accessibility to maintain a system or components should be stated in the contract.

Maintenance policies should be refined and augmented at each tier. At Tier 1, the policy should define allowed maintenance activities. At Tier 2, the policy should reflect the mission operations needs, and at Tier 3, it should reflect the specific system needs. The requirements in Tier 1, such as nonlocal maintenance, should flow to Tiers 2 and 3; for example, when nonlocal maintenance is not allowed by Tier 1, it should also not be allowed at Tiers 2 and 3.

TIER: 1,2,3

SCRM_MA-2 CONTROLLED MAINTENANCE

Control Enhancements:

(1) *CONTROLLED MAINTENANCE |AUTOMATED MAINTENANCE ACTIVITIES* *MA-2 (2)*

Supplemental ICT SCRM Guidance: Within the ICT SCRM context, automated maintenance activities include suppliers' patch updates. These are either automatically triggered by the software call-home feature or can be triggered by the user. Organizations should expressly select whether and how these mechanisms are used. A staging process with appropriate supporting mechanisms should be established to ensure that appropriate acceptance testing is completed before maintenance upgrades or updates are installed on an operational system.

TIER: 3

SCRM_MA-3 MAINTENANCE TOOLS **MA-3**

Supplemental ICT SCRM Guidance: Maintenance tools have an ICT supply chain of their own. When maintenance tools are introduced and upgraded, organizations should consider supply chain security implications of this set of actions. This is applicable when there is a need to acquire or upgrade a maintenance tool (e.g., an update to development environment or testing tool), including the selection, ordering, storage, and integration of the maintenance tool. This should include replacement parts for maintenance tools. This activity may be performed at both Tiers 2 and 3, depending on how an agency handles the acquisition, operations, and oversight of maintenance tools.

TIER: 2, 3.

Control Enhancements:

(1) *MAINTENANCE TOOLS | INSPECT TOOLS* *MA-3(1)*

Supplemental ICT SCRM Guidance: Organizations should deploy acceptance testing to verify that the maintenance tools are as expected and provide only required functions. Maintenance tools should be authorized with appropriate paperwork, verified as claimed through initial verification, and then acceptance tested for stated functionality.

TIER: 3

(2) *MAINTENANCE TOOLS | INSPECT MEDIA* MA-3(2)

Supplemental ICT SCRM Guidance: None.

TIER: 3

(3) *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL* *MA-3(3)*

Supplemental ICT SCRM Guidance: Removal of maintenance tools introduces an ICT Supply Chain risk including, for example, unauthorized modification, replacement with counterfeit, or malware insertion while the tool is outside of the organization's control. For ICT SCRM, it is important that organizations should explicitly authorize, track, and audit any removal of maintenance tools.

TIER: 3

SCRM_MA-4 NON-LOCAL MAINTENANCE **MA-4**

TIER: 2, 3.

Control Enhancements:

(1) *NON-LOCAL MAINTENANCE | DOCUMENT NON-LOCAL MAINTENANCE* *MA-4(2)*

Supplemental ICT SCRM Guidance: Organizations should deploy acceptance testing to verify that the maintenance tools are as expected and provide only required functions. Maintenance tools should be authorized with appropriate paperwork, verified as claimed through initial verification, and then acceptance tested for stated functionality.

TIER: 2, 3

(2) *NON-LOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION* *MA-4(3)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(3) *NON-LOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS* *MA-4(5)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

SCRM_MA-5 MAINTENANCE PERSONNEL MA-5

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

SCRM_MA-6 TIMELY MAINTENANCE MA-6

Supplemental ICT SCRM Guidance: For spare parts, replacement parts, or alternate sources, agencies should ensure appropriate lead-times to purchase through original equipment manufacturer (OEM)s or authorized distributors. If OEMs are not available, it is preferred to acquire from authorized distributors. If OEM or an authorized distributor is not available and the only alternative is to purchase from a non-authorized distributor or secondary market, a risk assessment should be performed to identify additional risk mitigations to be used. For example, the acquirer should check for history of counterfeits, inappropriate practices, or a criminal record.

TIER: 3

SCRM_MA-7 MAINTENANCE MONITORING AND INFORMATION SHARING

Control: The organization monitors the status of systems and components and communicates out of bounds and out of spec performance to [Assignment: organization-defined system integrators, suppliers, or external service providers].

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

Related Control: IR-4(10)

TIER: 3

FAMILY: MEDIA PROTECTION

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

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

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

SCRM_MP-1 MEDIA PROTECTION POLICY AND PROCEDURES MP-1

Supplemental ICT SCRM Guidance: A number of documents and information on a variety of physical and electronic media is disseminated across the ICT supply chain. This information contains a variety of acquirer, system integrator, supplier, and external service provider sensitive information and intellectual property. Because the media traverses or resides in the ICT supply chain, it is especially important to protect it. Media protection policies and procedures should address media in the federal agency acquirer's ICT supply chain.

TIER: 1,2

SCRM_MP-2 MEDIA TRANSPORT MP-5

Supplemental ICT SCRM Guidance: Organizations should consider ICT supply chain risks when transporting media, either by acquirer or non-acquirer personnel or organizations. Some of the techniques to protect media during transport and storage include cryptographic techniques and approved custodian services.

TIER: 1,2

SCRM_MP-3 MEDIA SANITIZATION MP-6

Control Enhancements:

(1) *MEDIA SANITIZATION | REVIEW/APPROVE/TRACK/DOCUMENT/VERIFY* *MP-6 (1)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(2) *MEDIA SANITIZATION | EQUIPTMENT TESTING* *MP-6 (2)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(3) *MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES* *MP-6 (3)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(4) *MEDIA SANITIZATION | DUAL AUTHORIZATION* *MP-6 (7)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

(5) *MEDIA SANITIZATION | REMOTE PURGING/ WIPING OF INFORMATION* *MP-6 (8)*

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

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

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

ICT supply chains span the physical and logical world. Physical factors including, for example, weather and road conditions that may have an impact to transporting ICT components (or devices) from one location to another between system integrators, suppliers, and organizations. If not properly addressed as a part of the ICT SCRM risk management processes, physical and environmental risks may have a negative impact on the federal agency acquirer's ability to receive critical components in a timely manner, which may in turn impact their ability to perform mission operations. Organizations should integrate physical and environmental protection controls to mitigate such risks and ensure that there are no gaps. It should be noted that the degree of physical and environmental protection required throughout the ICT supply chain is greatly dependent on the degree of integration between acquirer and system integrator/supplier/external service provider organizations, systems, and processes.

SCRM_PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES PE-1

Supplemental ICT SCRM Guidance: Organizations should integrate ICT supply chain risks into physical and environmental protection policy. The degree of such protection required throughout the ICT supply chain is greatly dependent on the degree of integration between acquirer and system integrator/supplier/external service provider organizations, systems, and processes. The physical and environmental protection policy should ensure that the physical interfaces have adequate protection and audit of such protection.

TIER: 1, 2, 3

SCRM_PE-2 PHYSICAL ACCESS CONTROL PE-3

Supplemental ICT SCRM Guidance: Ensure that physical access control covers individuals and organizations engaged in the organizations' ICT supply chain such as system integrator, supplier, and external service provider personnel.

TIER: 2,3

Control Enhancements:

(1) *PHYSICAL ACCESS CONTROL | TAMPER PROTECTION* PE-3 (5)

Supplemental ICT SCRM Guidance: None.

TIER: 2, 3

SCRM_PE-3 MONITORING PHYSICAL ACCESS PE-6

Supplemental ICT SCRM Guidance: None.

TIER: 3

SCRM_PE-4 DELIVERY AND REMOVAL PE-16

Supplemental ICT SCRM Guidance: None.

TIER: 3

SCRM_PE-5 ALTERNATE WORK SITE PE-17

Supplemental ICT SCRM Guidance: Organizations should consider the risks associated with system integrator personnel using alternate work sites.

TIER: 3

SCRM_PE-6 LOCATION OF INFORMATION SYSTEM COMPONENTS PE-18

Supplemental ICT SCRM Guidance: Physical and environmental hazards have an impact on the availability of systems and components that are or will be acquired and physically transported to the federal agency acquirer locations. For example, organizations should consider location of information system components critical for agency operations when planning for alternative suppliers for these components. See CP-6 and CP-7

TIER: 1, 2, 3

Control Enhancements:

(1) *LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE* PE-18 (1)

Supplemental ICT SCRM Guidance: None.

TIER: 1, 2, 3

SCRM_PE-7 INFORMATION LEAKAGE PE-19

Supplemental ICT SCRM Guidance: None.

TIER: 3

SCRM_PE-8 ASSET MONITORING AND TRACKING PE-20

Supplemental ICT SCRM Guidance: Organizations should use asset location technologies to track system and components transported between protected areas, or in storage awaiting implementation, testing, maintaining, or disposal. These technologies help protect against:

a. Diverting system or component for counterfeit replacement;
b. Loss of confidentiality, integrity or availability of system or component function and data (including data contained within the component and data about the component); and
c. Interrupting supply chain and logistics processes for critical components.

Asset location technologies also help gather data that can later be used for incident management.

TIER: 2, 3

FAMILY: SECURITY PLANNING

FIPS 200 specifies the Planning minimum security requirement as follows:

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

ICT SCRM concerns should influence security planning, including such activities as security architecture, coordination with other organizational entities, and development of System Security Plans. When acquiring ICT products and services from system integrators, suppliers, and external service providers, organizations may be sharing facilities with those organizations, having employees of these organizations on the federal agency premises, or use information systems that belong to those entities. In these and other applicable situations, organizations should coordinate their security planning activities with these entities to ensure appropriate protection of federal agency ICT supply chain infrastructure, as well as of the systems traversing the ICT supply chain. When establishing security architectures, organizations should provide for component and supplier diversity to manage the ICT supply chain-related risks of suppliers going out of business or stopping the production of specific components. Finally, as stated in Chapter 2, organizations may integrate ICT SCRM controls into System Security Plans for individual systems.

SCRM_PL-1 SECURITY PLANNING POLICY AND PROCEDURES PL-1

Supplemental ICT SCRM Guidance: Include ICT supply chain risk management considerations in security planning policy and procedures. This should include security policy, operational policy, and procedures for ICT supply chain risk management to shape the requirements and the follow-on implementation of operational systems.

TIER: 1

SCRM_PL-2 SYSTEM SECURITY PLAN PL-2

Supplemental ICT SCRM Guidance: Include ICT supply chain considerations in the System Security Plan. It is also acceptable to develop a stand-alone ICT SCRM Plan for an individual system. System Security Plan and/or ICT SCRM Plan provide inputs into ICT SCRM Plan(s) at Tier 1 and Tier 2 (Chapter 2 provides guidance on ICT SCRM Plan.). To include ICT SCRM in System Security Plan, controls listed in this document (NIST SP 800-161) should be used. Examples of systems that are important for ICT supply chain include acquirer’s development environment, testing environment and other systems that support acquirer’s ICT supply chain activities.

TIER: 3

Control Enhancements:

(1) *SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES* PL-2 (3)

Supplemental ICT SCRM Guidance: Include ICT supply chain security activities in coordination with other organizational entities. In this context, in addition to coordinating within the organization, other acquirers should coordinate with system integrators, suppliers, and external service providers. For example, building and operating a system requires a significant amount of coordination and collaboration between acquirer and system integrator personnel. This coordination and collaboration should be addressed in the System Security Plan. System Security Plans should also take into account that suppliers or external service providers may not be able to customize to the acquirer's requirements.

TIER: 2

SCRM_PL-3 INFORMATION SECURITY ARCHITECTURE **PL-8**

Supplemental ICT SCRM Guidance: Include ICT supply chain considerations in security architecture. Security architecture and its development, maintenance/update, and documentation for base-lining have significant ICT supply chain impacts. Defining and building security architecture is performed at Tier 2 and may require the evaluation and test of multiple components. Security architecture will be implemented in Tier 3 within individual systems. However, security architecture is also influenced by Tier 1 organization policy/procedures. In Tier 3, the security architecture of a system is impacted by the acquirers' operational enterprise security infrastructure such as encryption protocols (IPSE/VPN, TLS/SSL, etc.), standard network protocols, IdAM, and Gateway/firewall/IPS implementations. Security architecture is important for ICT SCRM because it defines and directs implementation of security methods, mechanisms, and capabilities which, in turn, define ICT components to be acquired.

TIER: 2, 3

Control Enhancements:

(1) *INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY* *PL-8(2)*

Supplemental ICT SCRM Guidance: Include supplier diversity when building security architecture. Supplier diversity is key to providing options for addressing information security and ICT supply chain concerns. This guidance must consider system integrators, suppliers, and external service providers.

When acquiring system integrator services, plan for potential replacement system integrators or external service providers in case a system integrator is no longer able to meet requirements (e.g., company goes out of business). For suppliers, plan for alternate sources of supply in case a supplier is no longer able to meet requirements.

Consider supplier diversity for off-the-shelf (commercial, government, or open source) components. Alternatives evaluation should include, for example, feature parity, standards interfaces, commodity components, and multiple delivery paths.

TIER: 2, 3

FAMILY: PROGRAM MANAGEMENT

FIPS 200 does not specific Program Management minimum security requirements.

NIST SP 800-53 Rev4 states that “the information security program management controls … are typically implemented at the organization level and not directed at individual organizational information systems.” Those controls apply to the entire organization (i.e., federal agency) and support the overall federal agency information security program. Program management controls support ICT SCRM risk management for the enterprise and provide inputs and feedback to ICT SCRM activities enterprise-wide.

SCRM_PM-1 INFORMATION SECURITY PROGRAM PLAN PM-1

Supplemental ICT SCRM Guidance: As a part of information security program planning, document common ICT SCRM controls. A separate ICT SCRM Plan may be developed to document common ICT SCRM controls to address organization, program, and system-specific needs. Information security program plan and the associated common controls addressing Tiers 1 and 2 can provide additional foundational practices to support the ICT SCRM Plan. For Tier 3, use the existing system security plan to incorporate ICT SCRM controls or develop a separate ICT SCRM Plan. In Tier 3, ensure that the full SDLC is covered from the ICT supply chain perspective.

TIER: 1,2,3

SCRM_PM-2 SENIOR INFORMATION SECURITY OFFICER PM-2

Supplemental ICT SCRM Guidance: Ensure that senior information security officer responsibilities include ICT SCRM and required cross-organizational coordination and collaboration with other senior personnel within the organization such as the CIO, the head of facilities/physical security, and the risk executive (function).

TIER: 1,2,3

SCRM_PM-3 INFORMATION SECURITY RESOURCES PM-3

Supplemental ICT SCRM Guidance: Ensure that ICT supply chain requirements are integrated into major IT investments to ensure that the funding is appropriately allocated through the capital planning and investment request process.

TIER: 1,2,3

SCRM_PM-4 MISSION/BUSINESS PROCESS DEFINITION PM-11

Supplemental ICT SCRM Guidance: When addressing business/mission process definitions, ensure ICT supply chain activities are incorporated into the support processes for achieving the mission process.

TIER: 2

SCRM_PM-5 THREAT AWARENESS PROGRAM PM-16

Supplemental ICT SCRM Guidance: When addressing supply chain threat event and threat awareness, knowledge is shared while within the boundaries of organization-specific policy information sharing of threat data/information.

Tier: 2

FAMILY: PERSONNEL SECURITY

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

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

Personnel that have access to federal agency ICT supply chain should be covered by federal agency personnel security controls. These personnel include acquisition and contracting professionals, program managers, supply chain and logistics professionals, shipping and receiving staff, information technology professionals, quality professionals, mission and business owners, system owners, and information security engineers. organizations should also work with system integrators and external service providers to ensure that they apply appropriate personnel security controls to their personnel that interact with the federal agency ICT supply chain, as appropriate.

SCRM_PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES PS-1

Supplemental ICT SCRM Guidance: At each tier, Personnel Security policy and procedures need to define the roles for the acquirer personnel who manage and execute ICT supply chain security activities. These roles also need to state acquirer personnel responsibilities with regards to the relationships with system integrators, suppliers, and service providers. Policies and procedures need to consider the full life cycle of systems, and the roles and responsibilities to address the various supply chain activities.

Tier 1: Include such roles as the risk executive, CIO, CISO, contracting, logistics, delivery/receiving, and other functions providing supporting ICT supply chain activities.

Tier 2: Include such roles as program executive, individuals within the acquirer organization responsible for program success (e.g., Program Manager and other individuals).

NOTE: Roles for system integrator, supplier, and external service provider personnel responsible for the success of the program should be included in an agreement between acquirer and these parties (e.g., contract). This is addressed in SA-4.

Tier 3: include applicable roles throughout the operational system life cycle from requirements definition, development, test, deployment, maintenance, updates, replacements, delivery/receiving, and IT.

TIER: 1,2,3

SCRM_PS-2 ACCESS AGREEMENTS PS-6

Supplemental ICT SCRM Guidance: Define and document access agreements for system integrators, external service providers, and suppliers. Access agreements should state appropriate level of access by system integrators, external providers, and suppliers to the acquirer's systems and should be consistent with the acquirer information security policy. Deploy audit mechanisms to review, update, and track access by these parties in accordance with the access agreement. As personnel vary over time, implement a timely and rigorous update process for the access agreements.

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

NOTE: When ICT products and services are provided by an entity within acquirer's organization, there may be an existing access agreement in place. When such agreement does not exist, it should be established.

TIER: 2

SCRM_PS-3 THIRD-PARTY PERSONNEL SECURITY PS-7

Supplemental ICT SCRM Guidance:

TIER: 2

FAMILY: PROVENANCE

Provenance is a new control family, developed specifically to address ICT supply chain concerns.

All systems and components originate somewhere and may be changed throughout their existence. The record of system and component origin along with the history of, the changes to, and the record of who made those changes is called “provenance.” Acquirers, system integrators, suppliers, and external service providers should maintain the provenance of systems and components under their control to understand where the systems and components have been, the change history, 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 systems and components to be reported to specific stakeholders. Creating and maintaining provenance within the ICT supply chain helps achieve greater traceability in case of an adverse event and is critical for understanding and mitigating risks.

SCRM_PV-1 Provenance Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates the provenance policy and procedures for [Assignment: organization-defined systems, or components that make up the ICT supply chain infrastructure, or components traversing the ICT supply chain]. The policy procedures should address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to support managing the information and documentation describing systems/components within ICT supply chain systems or within those systems traversing the ICT supply chain; and
b. Reviews and updates the current organization or mission provenance policy and procedures every [*Assignment: organization-defined frequency*].

Supplemental ICT SCRM Guidance: Provenance policy can be included in the overall information security policy for organizations or conversely, can be represented by multiple program security policies reflecting the complex nature of federal agencies. The procedures can be established for the security program in general and for individual information systems, if needed.

The provenance policy should 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 that of the individual items for which provenance is maintained. It should include:

a. Procedures for proposing, evaluating, and justifying relevant changes to system/component provenance for their impact on components, processes, systems, missions, and exposure to supply chain risks;
b. Allocation of responsibilities for the creation, maintenance, and monitoring of provenance are documented;
c. Methods for tracking relevant purchasing, shipping, receiving, or transfer activities, including records of reviewer signatures for comparison;
d. Processes for transferring provenance responsibility for systems or components between organizations across physical and logical boundaries including any approvals required, e.g., from system integrator or supplier to acquirer. This may include the identification of key personnel for the handling of information; and
e. Procedures for tracking and documenting chain of custody of the system or component.

TIER: 1, 2, 3

SCRM_PV-2 Tracking Provenance and Developing a Baseline

Control: The organization:

a. Provides unique identification for the provenance document for tracking as it traverses the ICT supply chain;
b. Develops methods to document, monitor, and maintain valid provenance baselines for systems and components of the ICT supply chain system or those system and components traversing the ICT supply chain;
c. Tracks, documents and disseminates to relevant supply ICT chain participants changes to the provenance;
d. Tracks individuals and processes that have access and make changes to the provenance of components, tools, data, and processes in ICT supply chain systems or those systems traversing the ICT supply chain; and
e. Ensures that the provenance information and the provenance change records including to whom, when, and what, is non-repudiable.

Supplemental ICT SCRM Guidance: Tracking of provenance helps to detect unauthorized tampering and modification throughout the ICT supply chain, especially during repairs/refurbishing, for example, by comparing the updated provenance with the original baseline provenance. Tracking of provenance baselines should be performed through using configuration management mechanisms. organizations should ensure the timely collection of provenance and change information to provide near real-time traceability as possible.

Examples include documenting, monitoring, and maintaining valid baselines for spare parts, development changes, and warehoused items throughout the SDLC.

TIER: 2, 3

Control Enhancements:

(1) *TRACKING PROVENANCE AND DEVELOPING A BASELINE| AUTOMATED AND REPEATABLE PROCESSES*

Supplemental ICT SCRM Guidance: Organizations should use a variety of repeatable methods for tracking changes to provenance including number and frequency of changes, reduction of "on/off" processes and procedures, and human error. These methods can be both manual and automated. For example, configuration management databases can be used for the tracking of changes to software modules, hardware components, and documentation.

Related Controls: *CM-3, CM-5, CM-6, CM-6 (1), CM-6 (2), CM-8, CM-8 (4), CM-8 (6), CM-8 (7), CM-8 (8), CM-8 (9), CM-9, CM-10 (1), CM-11, SA-12 (14)*

TIER: 3

SCRM_PV-3 Auditing Roles Responsible for Provenance

Control: The organization:

1) Audits and verifies provenance activities performed by [Assignment: Organization-defined individuals granted access to the creation, maintenance or monitoring of provenance]; and
2) Protects provenance audit records.

Supplemental ICT SCRM Guidance: These may include both automated and manual systems. Audits of provenance should be performed through using access control and audit mechanisms.

TIER: 2, 3

RELATED CONTROLS: AU -10 (1), AU -10 (2), AU -10 (3), AU -10 (4),SA-12 (11)

FAMILY: RISK ASSESSMENT

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

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

NIST SP 800-161 is about managing federal agency ICT supply chain risks and expands this control to integrate ICT supply chain risk assessment activities, as described in Chapter 2.

SCRM_RA-1 RISK ASSESSMENT POLICY AND PROCEDURES RA-1

Supplemental ICT SCRM Guidance: Risk assessment should be performed at the organization, mission/program, and system levels. The system-level risk assessment should include both the systems providing ICT supply chain capabilities (e.g., development environments, test, or delivery systems) and the systems traversing the ICT supply chain. The policy should include ICT supply chain-relevant roles applicable to performing and coordinating risk assessments across the organization (see Chapter 2 for the listing and description of roles). Applicable roles within acquirer, system integrator, external service providers, and supplier organizations should be defined.

TIER: 1,2,3

SCRM_RA-2 SECURITY CATEGORIZATION RA-2

Supplemental ICT SCRM Guidance: Security categorization is critical to ICT SCRM at Tiers 1, 2, and 3. In addition to FIPS 199, for ICT SCRM, security categorization should be based on the criticality analysis (See Chapter 2 and SA-15[3] for a more detailed description of criticality analysis.).

TIER: 1,2, 3

SCRM_RA-3 RISK ASSESSMENT RA-3

Supplemental ICT SCRM Guidance: Conduct risk assessment with the consideration of ICT supply chain criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Chapter 2 (Integration of ICT SCRM into Risk Management). Data to be reviewed and collected includes ICT SCRM-specific roles, processes, and results of system/component implementation and acceptance. Risk assessments should be performed at Tiers 1 and 2.

Risk assessment at Tier 1 should be primarily a synthesis of various risk assessments performed at Tiers 2 and 3 for understanding the organizational impact.

TIER: 1,2,3

FAMILY: SYSTEM AND SERVICES ACQUISITION

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

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

System and services acquisition is how federal agencies acquire ICT products and services. These controls address federal agency acquisition activities, as well as the system integrator, supplier, and external service provider activities. They address both physical and logical aspects of ICT supply chain security, from tamper resistance and detection to SDLC and security engineering principles. ICT supply chain concerns are already prominently addressed in NIST SP 800-53 Rev4. NIST SP 800-161 adds further detail and refinement to these controls.

SCRM_SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES SA-1

Supplemental ICT SCRM Guidance: Organizations should make sure that their system and services acquisition policy addresses ICT SCRM including changes of location, ownership, and control, and requirements to be communicated to the ICT supply chain. ICT supply chains evolve continuously through mergers and acquisitions, joint ventures, and other partnership agreements. The policy should help organizations understand these changes and use this information within their ICT SCRM activities. Organizations can obtain such status through, for example, monitoring public announcements about company activities or any communications initiated by system integrator, supplier, or external service provider.

TIER: 1,2,3

SCRM_SA-2 ALLOCATION OF RESOURCES SA-2

Supplemental ICT SCRM Guidance: Organizations should include ICT supply chain requirements in the allocation of resources.

TIER: 1,2

SCRM_SA-3 SYSTEM DEVELOPMENT LIFE CYCLE SA-3

Supplemental ICT SCRM Guidance: Organizations should ensure that ICT supply chain security considerations are integrated into the SDLC for ICT supply chain systems and those systems traversing the ICT supply chain. There is a strong relationship between the SDLC activities and ICT supply chain activities. Organizations should ensure that in addition to traditional SDLC activities, such as requirements and design, less traditional activities are also considered in the SDLC, such as inventory management, acquisition and procurement, and logical delivery of systems and components. See Chapter 2.

TIER: 1, 2, 3

SCRM_SA-4 ACQUISITION PROCESS SA-4

Supplemental ICT SCRM Guidance: To integrate ICT SCRM into the federal agency acquisition process, organizations should ensure that the following acquisition-related requirements, descriptions, and criteria are addressed:

a. Establish a baseline and tailor-able ICT supply chain security requirements to apply to all system integrators, suppliers, and external service providers;
b. Define requirements that cover regulatory requirements (i.e., telecommunications or IT), technical requirements, chain of custody, transparency and visibility, sharing information on information and supply security incidents throughout the supply chain, rules for disposal or retention of elements such as components, data, or intellectual property, and other relevant requirements;
c. Define requirements for critical elements in the ICT supply chain to demonstrate a capability to remediate emerging vulnerabilities based on information gathered and other sources;
d. Identify requirements for managing intellectual property ownership and responsibilities for elements such as software code, data and information, the manufacturing/development/integration environment, designs, and proprietary processes when provided to acquirer for review or use;
e. Define requirements for the expected life span of the system and which element may be in the critical path based on their life span. Establish a plan for any migration that can be required in support of continued system and mission operations to ensure that the supplier relationship can provide insights into their plans for end-of-life components. Establish a plan for acquisition of spare parts to ensure adequate supply;
f. Define requirements for an established system integrator, supplier, external service provider vulnerability response process and their capability to collect inputs on vulnerabilities from acquirers and other organizations;
g. Establish and maintain verification procedures and criteria for delivered products and services;
h. Monitor system integrators, suppliers, and external service providers' information systems where applicable. Monitor and evaluate the acquired work processes and work products where applicable;
i. Report information security weakness and vulnerabilities detected in the use of ICT products or services provided within the acquirer organization and to respective OEMs where relevant;
j. Review and confirm that the delivered product or service complies with the agreement on an ongoing basis; and
k. Articulate circumstances when secondary market components are permitted, if they are.

TIER: 1, 2, 3

Control Enhancements:

(1) *ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS* *SA-4 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS* *SA-4 (5)*

Supplemental ICT SCRM Guidance: If a federal agency acquirer needs to purchase components, they need to ensure that the required item meets its specification, whether purchasing directly from the OEM, channel partners, or secondary market.

TIER: 3

(3) *ACQUISITION PROCESS | NIAP APPROVED PROTECTION PROFILES* *SA-4 (7)*

Supplemental ICT SCRM Guidance: Organizations should build, procure, and or use U.S. government protection profile-certified components. NIAP certification can be achieved for OTS (COTS, Open Souce Software (OSS), GOTS).

TIER: 2, 3

(4) *ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN* SA-4 (8)

Supplemental ICT SCRM Guidance: See Chapter 2, NIST SP 800-161.

TIER: 2

(5) *ACQUISITION PROCESS | FUNCTIONS/PORTS/PROTOCOLS IN USE* SA-4 (9)

Supplemental ICT SCRM Guidance: None

TIER: 2

SCRM_SA-5 INFORMATION SYSTEM DOCUMENTATION **SA-5**

Supplemental ICT SCRM Guidance: Federal agency acquirer should integrate ICT supply chain concerns into information system documentation.

TIER: 3

SCRM_SA-6 SECURITY ENGINEERING PRINCIPLES SA-8

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

a. Anticipating maximum possible ways the ICT product or service can be misused and abused or to protect the product or system from such uses. Addressing intended and unintended use scenarios in architecture and design;
b. Designing based on the federal agency acquirer's risk tolerance;
c. Documenting acceptance of risks that are not fully mitigated through management acceptance and approval;
d. Limiting the number, size, and privileges of critical elements;
e. Using security mechanisms that help reduce opportunities to exploit ICT supply chain vulnerabilities, including, for example, encryption, access control, identity management, and malware or tampering discovery;
f. Designing components elements to be difficult to disable and, if disabled, trigger notification methods such as audit trails, tamper evidence; or alarms;
g. Designing delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or access to the ICT supply chain and the systems/components traversing ICT supply chain during delivery; and
h. Designing relevant validation mechanisms to be used during implementation and operation.

TIER: 1, 2, 3

SCRM_SA-7 EXTERNAL INFORMATION SYSTEM SERVICES SA-9

TIER: 1, 2, 3

Control Enhancements:

(1) *EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS* SA-9 (1)

Supplemental ICT SCRM Guidance: See Chapter 2, Assess and Appendices E and F.

TIER: 2, 3

(2) *EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN CHAIN OFTRUST WITH PROVIDERS* SA-9 (3)

Supplemental ICT SCRM Guidance: Organizations should ensure that their relationships with external service providers of information systems, whether a system integrator or an external service provider, meet the following supply chain security requirements:

a. Ensure requirements definition is complete and reviewed for accuracy and completeness including the assigning of criticality to various components as well as defining operational concepts and associated scenarios for intended and unintended use in requirements,
b. Ensure requirements are based on needs, relevant compliance drivers, and ICT supply chain and system risk assessment,
c. Identify and document threats, vulnerabilities, and associated risks based on likelihood and impact for the defined system, component, and processes used across the system's SDLC,
d. Ensure acquirer data and information integrity, confidentiality, and availability requirements are defined and shared with system integrator/external service provider as appropriate, for compliance to requirement,
e. Define and document consequences of noncompliance with ICT supply chain security requirements and information security requirements for ICT product and service delivery; and
f. Define requirements for service contracts completion and what defines the end of the system integrator/external supplier relationship. This is important to know for acquirer recompete and potential change in service provider and also to manage system end-of-life processes.

TIER: 1, 2, 3

(3) *EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS* SA-9 (4)

Supplemental ICT SCRM Guidance: None

TIER: 3

(4) *EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION* SA-9 (5)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SA-8 DEVELOPER CONFIGURATION MANAGEMENT

Control Enhancements:

(1) *DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION* SA-10 (1)

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES* SA-10 (2)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION* SA-10 (3)

Supplemental ICT SCRM Guidance: None

TIER: 3

(4) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION* SA-10 (4)

Supplemental ICT SCRM Guidance: None

TIER: 3

(5) *DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL* SA-10 (5)

Supplemental ICT SCRM Guidance: None

TIER: 3

(6) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION* SA-10 (6)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SA-9 DEVELOPER SECURITY TESTING SA-11

Supplemental ICT SCRM Guidance: Depending on the origins of components, this control may be implemented differently. For OTS (off-the-shelf) components, the acquirer should request proof that the supplier (OEM) has performed such testing as part of their quality/security processes. When the acquirer has control over the application and the development processes, they should require this testing as part of the SDLC. In addition to the specific types of testing activities described in the enhancements, examples of ICT SCRM-relevant testing include testing for counterfeits, testing the origins of components, examining configuration settings prior to integration, and testing the interfaces. These types of tests may require significant resources and should be prioritized based on the system criticality analysis (described in Chapter 2) and effectiveness of testing techniques. Organizations may also require third-party testing as part of developer security testing.

TIER: 1, 2, 3

Control Enhancements:

(1) *DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS* SA-11 (1)

Supplemental ICT SCRM Guidance: None

TIER: 3

(2) *DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES* SA-11 (2)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE* SA-11 (3)

Supplemental ICT SCRM Guidance: None

TIER: 3

(4) *DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS* SA-11 (4)

Supplemental ICT SCRM Guidance: None

TIER: 3

(5) *DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS* SA-11 (5)

Supplemental ICT SCRM Guidance: None

TIER: 3

(6) *DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS* SA-11(6)

Supplemental ICT SCRM Guidance: None

TIER: 3

(7) *DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION* SA-11(7)

Supplemental ICT SCRM Guidance: None

TIER: 3

(8) *DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE* SA-11(8)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SA-10 SUPPLY CHAIN PROTECTION SA-12

Supplemental ICT SCRM Guidance: NIST SP 800-161 addresses supply chain protection.

TIER: 1, 2, 3

Control Enhancements:

(9) *SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS* SA-12 (1)

Supplemental ICT SCRM Guidance: None

TIER: 1, 2, 3

(10) *SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS* SA-12 (2)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(11) *SUPPLY CHAIN PROTECTION | LIMITATION OF HARM* SA-12 (5)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(12) *SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE* *SA-12 (7)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(13) *SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE* *SA-12 (8)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(14) *SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY* *SA-12(9)*

TIER: 2, 3

(15) *SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED* *SA-12(10)*

Supplemental ICT SCRM Guidance: Examples of unauthorized modifications include the deployment of a patch or an upgrade by a maintenance team prior to staging processes to verify impact of upgrade to operational environment.

TIER: 2, 3

(16) *SUPPLY CHAIN PROTECTION | PENETRATION TESTING/ANALYSIS OF ELEMENT* *SA-12(11)*

Supplemental ICT SCRM Guidance: Example of validation may be the use of digital signature by an OEM to prove that the software delivered is from its originating source. When digital signatures are used for this purpose, the federal agency acquirer should ensure, when receiving such software, that the signed upgrade/download was not altered.

TIER: 2, 3

(17) *SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS* *SA-12(12)*

Supplemental ICT SCRM Guidance: Federal agency acquirer should establish inter-organizational agreements with its system integrators, suppliers, and external service providers to ensure that appropriate resources and system components are available. Additional safeguards include:

a. Suppliers periodically communicating roadmaps to their OEM for new products and end of life;
b. Formally reviewing and approving system integrator adding or replacing personnel; and
c. Ensuring that external service providers provide appropriate notice regarding any infrastructure changes such as any new operating system rollout, hardware upgrades or replacements due to field failures, or data store architecture shifts from central to distribute.

TIER: 2, 3

(18) *SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS* *SA-12 (13)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(19) *SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY* *SA-12(14)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(20) *SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES* *SA-12(15)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SA-11 CRITICALICALITY ASSESSMENT **SA-14**

Supplemental ICT SCRM Guidance: For systems in architectural design, perform component-level security categorization to support the system-level criticality analysis to ensure confidentiality, integrity, or availability of the system and the mission it supports. See Chapter 2, Criticality Analysis.

TIER: 2, 3

SCRM_SA-12 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS SA-15

Supplemental ICT SCRM Guidance: Organizations should ensure that ICT supply chain systems (development process, standards, tools, etc.) are appropriately identified, analyzed for their criticality, and appropriately protected from insider attacks. Development/maintenance environment, test environment, and deployment environments are all critical.

TIER: 2, 3

Control Enhancements:

(1) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS* *SA-15 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS* *SA-15 (2)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS* *SA-15 (3)*

Supplemental ICT SCRM Guidance: See Chapter 2.

TIER: 2, 3

(4) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS* *SA-15 (4)*

SCRM Guidance: See Chapter 2, Appendices E and F, and the SCEFOR

TIER: 2, 3

(5) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION* SA-15 (5)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(6) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT* SA-15 (6)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(7) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS* SA-15 (7)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(8) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION* SA-15 (8)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SA-13 DEVELOPER-PROVIDED TRAINING SA-16

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

Control Enhancements:

(1) *TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION* SC-16 (1)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SA-14 DEVELOPER-PROVIDED TRAINING

Control Enhancements:

(1) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL* SA-17 (1)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE* SA-17 (3)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SA-15 TAMPER RESISTANCE AND DETECTION SA-18

Supplemental ICT SCRM Guidance: Organizations can use tamper-resistance techniques to reduce counterfeit and tampering software and hardware in the ICT supply chain. Examples of tamper-resistance techniques include retarring of chips to avoid rebranding of discarded chips, or digital signatures to help non-repudiation of software.

TIER: 1, 2, 3

Control Enhancements:

(1) *TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC* *SA-18(1)*

Supplemental ICT SCRM Guidance: To ensure ICT components are not salvaged, reclaimed, otherwise used, or previously rejected for any reason, organizations may require documentation (certifications, packing slips, etc.) that is continuous in that it enables the tracing of handling and delivery back to the supplier (OEM).

TIER: 2, 3

(2) *TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES* *SA-18 (2)*

Supplemental ICT SCRM Guidance: Organizations should examine inconsistencies among different types of tracking and labeling of delivered ICT components to identify counterfeit components, for example:

a. Mismatched lot and the date code;
b. Absent or mismatched manufacturers logo and label on the ICT component and its documentation;
c. Mismatched bar code and printed part number; and
d. Inconsistent descriptions between package materials and datasheet descriptions.

These comparisons can be done via visual inspections, or a variety of pattern-matching techniques used in supply chain logistics.

TIER: 2, 3

(3) *TAMPER RESISTANCE AND DETECTION | RETURN POLICY*

Supplemental ICT SCRM Guidance: Organizations should establish a return policy and procedures for ICT components with their suppliers including what approvals, tracking, and documentation is required for such returns. This should include returns of excess inventory of ICT hardware components.

TIER: 2, 3

SCRM_SA-16 COMPONENT AUTHENTICITY SA-19

Supplemental ICT SCRM Guidance: Organizations can use tamper-resistance techniques to reduce counterfeit and tampering software and hardware in the ICT supply chain. Examples of tamper-resistance techniques include retarring of chips to avoid rebranding of discarded chips, or digital signatures to help non-repudiation of software.

TIER: 2, 3

Control Enhancements:

(1) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING* *SA-19 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR* SA-19 (2)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *COMPONENT AUTHENTICITY | COMPONENT DISPOSAL* SA-19 (3)

Supplemental ICT SCRM Guidance: Organizations should ensure that ICT components can be disposed of without exposing organization, mission, or operational information which may lead to a future ICT supply chain compromise. This includes:

a. Considering the transmission of sensitive data (mission, user, operational system) to unauthorized parties or unspecified parties during disposal activities;
b. Monitoring and documenting the chain of custody through the destruction process;
c. Training disposal service personnel to ensure accurate delivery of service against disposal policy and procedure; and
d. Implementing assessment procedures for the verification of disposal processes with a frequency that fits organizational/mission needs.

TIER: 2, 3

(4) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING (SCANNING)* SA-19 (4)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SA-17 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS SA-20

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SA-18 DEVELOPER SCREENING SA-21

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

CONTROL ENHANCEMENTS:

(1) *DEVELOPER SCREENING| VALIDATION OF SCREENING* SA-21 (1)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SA-19 UNSUPPORTED SYSTEM COMPONENTS SA-22

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

Control Enhancements:

(1) *UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT* SA-22 (1)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

FAMILY: SYSTEM AND COMMUNICATION PROTECTION

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

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

Federal agency communication infrastructures are composed of ICT components and systems which have their own ICT supply chains and also support federal agency ICT supply chain infrastructure. These communications connect federal agency systems with system integrator and occasionally supplier systems. Federal agency communications may be provided by system integrators or external service providers.

SCRM_SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES SC-1

Supplemental ICT SCRM Guidance: Organizations should ensure that system and communications protection policies and procedures address ICT supply chain security perspective. The need for such protections include defining organization-level and program-specific policies which help to set the requirements of communication and how the infrastructure is established to meet these requirements. This can include the coordination of communications among and across multiple organizational entities within the acquirer organization as well as communications methods and infrastructure used between the acquirers and its system integrators, suppliers, and external service providers.

TIER: 1,2,3

SCRM_SC-2 INFORMATION IN SHARED RESOURCES SC-4

Supplemental ICT SCRM Guidance: The ICT supply chain security context of this control is when a federal agency acquirer shares information system resources with system integrators or external service providers.

TIER: 2,3

SCRM_SC-3 INFORMATION IN SHARED RESOURCES

CONTROL ENHANCEMENTS:

(1) *DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY* *SC-5 (2)*

Supplemental ICT SCRM Guidance: Organizations should include requirements for excess capacity, bandwidth, and redundancy into agreements with system integrators, external service providers, and suppliers of OEM equipment.

TIER: 2

SCRM_SC-4 BOUNDARY PROTECTION SC-7

Supplemental ICT SCRM Guidance: Organizations should implement appropriate monitoring mechanisms and processes at the boundaries between the agency systems and system integrator, supplier, and external services provider systems. There may be multiple interfaces throughout the federal agency ICT supply chain infrastructure and the SDLC.

TIER: 2

CONTROL ENHANCEMENTS:

(1) *BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS* SC-7 (13)

Supplemental ICT SCRM Guidance: Federal agency acquirer should provide separation and isolation of development, test, security assessment tools, and operational environments and relevant monitoring tools. Should a compromise or information leakage happen in any one of the environments, the other environments are still protected through the separation/isolation mechanisms or techniques.

TIER: 3

(2) *BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS* SC-7 (19)

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

TIER: 3

SCRM_ SC-5 TRANSMISSION CONFIDENTIALITY AND INTEGRITY SC-8

Supplemental ICT SCRM Guidance: Organizations should integrate requirements for transmission confidentiality and integrity into agreements with system integrators, suppliers, and external service providers. Acquirers, system integrators, suppliers, and external service providers may repurpose existing security mechanisms (e.g., authentication, authorization, or encryption) to achieve these requirements. The degree of protection should be based on the relationship between the acquirer and the other party as well as the sensitivity of information to be transmitted.

TIER: 2, 3

SCRM_SC-6 TRANSMISSION OF SECURITY ATTRIBUTES SC-16

CONTROL ENHANCEMENTS:

(1) *TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION* SC-16 (1)

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SC-7 MOBILE CODE SC-18

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

TIER: 3

CONTROL ENHANCEMENTS:

(1) *MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS* SC-18 (1)

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) MOBILE CODE | ACQUISITION / DEVELOPMENT / USE *SC-18 (2)*

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SC-8 PLATFORM-INDEPENDENT APPLICATIONS SC-27

Supplemental ICT SCRM Guidance: Organizations may consider using platform-independent applications for ICT SCRM to make the ICT SCRM application more resilient to changes in infrastructure.

TIER: 2, 3

SCRM_SC-9 PROTECTION OF INFORMATION AT REST SC-28

Supplemental ICT SCRM Guidance: Organizations should include provisions for protection of federal agency information at rest into their agreements with system integrators, suppliers, and external service providers. Conversely, organizations should also ensure that they provide appropriate protections for data at rest for the system integrator, supplier, and external service provider information, such as source code, testing data, blueprints, and intellectual property information. This control should be applied throughout the SDLC including during requirements, development, manufacturing, test, inventory management, maintenance and disposal.

TIER: 2, 3

SCRM_SC-10 HETEROGENEITY SC-29

Supplemental ICT SCRM Guidance: Organizations should consider using multiple sources of supply to improve component availability and reduce ICT supply chain compromise impact. Heterogeneity techniques include use of different operating systems, virtualization techniques, and multiple sources of supply for the same function. In case of an ICT supply chain compromise, an alternative source of supply will allow the federal agency acquirer to quickly switch to an alternative system/component which may not be affected by the compromise. Also, heterogeneous components decrease the attack surface by limiting the impact to only a subset of the infrastructure that is using vulnerable components.

TIER: 2, 3

CONTROL ENHANCEMENTS:

(1) HETEROGENEITY | VIRTUALIZATION TECHNIQUES *SC-29 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SC-11 CONCEALMENT AND MISDIRECTION SC-30

Supplemental ICT SCRM Guidance: Within ICT SCRM context, concealment and misdirection techniques include the establishment of random resupply times, concealment of location, random change of fake location used and in logical space, and random change/shifting of information storage into alternate servers/storage mechanisms.

TIER: 3

Control Enhancements:

(1) *CONCEALMENT AND MISDIRECTION | RANDOMNESS* *SC-30 (2)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS* *SC-30 (3)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(2) *CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION* *SC-30 (4)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

(3) *CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM / COMPONENTS* *SC-30 (5)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SC-12 INFORMATION SYSTEM PARTITIONING **SC-32**

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SC-13 DISTRIBUTED PROCESSING AND STORAGE **SC-36**

Supplemental ICT SCRM Guidance: Organizations should be aware that processing and storage can be distributed both across the ICT supply chain and across the SDLC and should ensure that these techniques are applied in both contexts. The following activities can use distributed processing and storage: development, manufacturing, configuration management, test, maintenance, and operations.

TIER: 2, 3

SCRM_SC-14 OUT-OF-BAND CHANNELS

CONTROL ENHANCEMENTS:

(1) *OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION* *SC-37 (1)*

Supplemental ICT SCRM Guidance: None

TIER: 2, 3

SCRM_SC-15 OPERATIONS SECURITY **SC-38**

Supplemental ICT SCRM Guidance: Organizations should ensure that appropriate ICT supply chain threat and vulnerability information is obtained from and provided to the operational security processes.

Tier 2, 3

FAMILY: SYSTEM AND INFORMATION INTEGRITY

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

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

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

SCRM_SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES SI-1

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

TIER: 1,2,3

SCRM_SI-2 FLAW REMEDIATION SI-2

Supplemental ICT SCRM Guidance: None

TIER: 2,3

CONTROL ENHANCEMENTS:

(1) *FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES* *SI- 2 (5)*
Supplemental ICT SCRM Guidance: Organizations should specify the various software assets within its infrastructure that require automated updates (both indirect and direct). Those that require direct updates from a supplier should only accept updates originating directly from the OEM unless specifically deployed by the acquirer, such as a centralized patch management process.

TIER: 2

SCRM_SI-3 MALICIOUS CODE PROTECTION SI-3

CONTROL ENHANCEMENTS:

(1) *MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS (TIER 3)* *SI-3 (8)*

Supplemental ICT SCRM Guidance: None

TIER: 2,3

SCRM_SI-4 INFORMATION SYSTEM MONITORING SI-4

Supplemental ICT SCRM Guidance: Information system monitoring is frequently performed by external service providers. Organizations should structure their service-level agreements with these providers to appropriately reflect this control. Additionally, this control includes monitoring of vulnerabilities resulting from past ICT supply chain compromises, such as malicious code implanted during software development that was set to activate after deployment.

TIER: 1,2,3

CONTROL ENHANCEMENTS:

(1) *INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION* *SI-4 (16)*

Supplemental ICT SCRM Guidance: None

TIER: 2,3

(2) *INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS* *SI-4 (17)*

Supplemental ICT SCRM Guidance: Organizations may correlate monitoring information with that of system integrators, suppliers, and external service providers, if appropriate. Additionally, the results of correlating monitoring information may point to ICT supply chain compromises.

TIER: 2,3

(3) *INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK* *SI-4 (19)*

TIER: 2,3

SCRM_SI-5 SECURITY ALERTS, ADVSORIES, AND DIRECTIVES **SI-5**

Supplemental ICT SCRM Guidance: None

TIER: 2,3

SCRM_SI-6 SECURITY FUNCTION VERIFICATION (TIER 2,3) **SI-6**

CONTROL ENHANCEMENTS:

(1) *SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION SI-6 (3)*

TIER: 2, 3

SCRM_SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (TIER 2,3) **SI-7**

Supplemental ICT SCRM Guidance: Within ICT SCRM context, this control applies to the supply chain systems and systems traversing the supply chain. Supply chain systems' integrity should be tested and verified to ensure that it remains as required so that the systems that are traversing through it are not impacted by unanticipated changes in the supply chain. Systems and components traversing the supply chain should be tested and verified that they are the way they are supposed to be. Applicable verification tools include digital signature verification of system updates, integrated development environment, static and dynamic analysis tools, or acceptance testing for physical components received by an organization.

TIER: 2, 3

CONTROL ENHANCEMENTS:

(1) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES* *SI-7(11)*

TIER: 2, 3

(2) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION* *SI-7(12)*

TIER: 2, 3

(3) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS* *SI-7(13)*

Supplemental ICT SCRM Guidance: None

TIER: 3

(4) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE* *SI-7(14)*

Supplemental ICT SCRM Guidance:: Organizations should obtain only binary or machine-executable code directly from the OEM or verified open source.

TIER: 2, 3

(5) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION* *SI-7 (15)*

Supplemental ICT SCRM Guidance: None

TIER: 3

SCRM_SI-8 INFORMATION OUTPUT HANDLING AND RETENTION SI-12

Supplemental ICT SCRM Guidance: ICT SCRM concerns should be included as operational requirements, especially when system integrator, supplier, and external service provider sensitive and proprietary information is concerned.

TIER: 3

APPENDIX A

GLOSSARY

Term	Definition	Source
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
Baseline Criticality	The identification of system and its components, whether physical or logical, that are considered critical to the federal agency acquirer mission. The reduced functional capability, incapacity, or destruction of such systems and components would have a significant adverse impact on federal agency operations (including mission, functions, image, or reputation), assets, individuals, other organizations, and the Nation.	Based on 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
Counterfeit (Goods)	An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source.	18 U.S.C. § 2320
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 retirement).	CNSSI-4009
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 that 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.	
External (information systems) Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.	NIST 800-53rev 4
Element	ICT system element member of a set of elements that constitutes a system.	
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
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 design of ICT products and services and extends through development, sourcing, manufacturing, handling and delivery of ICT products and services to the acquirer. Note: An ICT supply chain can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services.	ISO 28001, adapted
ICT SCRM Control	Means of managing ICT supply chain risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.	ISO/IEC 27000, adapted
ICT Supply Chain Compromise	An ICT supply chain compromise is an occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service. NOTE: System includes physical or electronic system or network of organizations, people, technology, activities, information, and resources. It also includes system or network components. In the context of ICT supply chain, system encompasses both the system that traverses the supply chain and organization's supply chain infrastructure. NOTE: ICT supply chain is system transforming natural resources, raw materials, and components into a finished ICT product or service from supplier to the end customer.	

	NOTE: Development life cycle in general includes design, manufacturing, production, distribution, acquisition, installation, operations, maintenance, and decommissioning.	
ICT Supply Chain Infrastructure	The integrated set of components (hardware, software and processes) within federal agency acquirer organizational boundary that compose the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned.	
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
ICT Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.	
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
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	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. 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). 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	CNSSI 4009

	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 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 monitoring of the security state of the information system.	NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37, adapted
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.	CNSSI-4009
Secondary market	An unofficial, unauthorized, or unintended distribution channel.	
Sources Sought Notice	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
ICT Supply Chain Logistics	The care, housing, and movement of ICT, including materials and components (hardware and software).	
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 Integrator	An organization that customizes (e.g., combines, adds, optimizes) components, systems, and corresponding processes. The integrator function can also be performed by acquirer.	NIST IR 7622, adapted

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/ Analysis	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	CNSSI-4009; SP 800-53A
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact.	NIST SP 800-30 Rev1
Threat Source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.	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.	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, and 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
APT	Advanced Persistent Threat
BIA	Business Impact Analysis
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPO	Chief Privacy Officer
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial Off-The-Shelf
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerability Enumeration
CWE	Common Weakness Enumeration
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act

GOTS	Government Off-The-Shelf
HAZMAT	Hazardous Materials
HR	Human Resources
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol/Intellectual Property
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
ITL	Information Technology Laboratory (NIST)
NSA	National Security Agency
NASPO	North American Security Products Organization
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NSTISSI	National Security Telecommunications and Information System Security Instruction
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OPSEC	Operations Security
OTS	Off-The-Shelf
O-TTPS	Open Trusted Technology Provider Standard
OWASP	Open Web Application Security Project
PACS	Physical Access Control System

PIV	Personal Identity Verification
PKI	Public Key Infrastructure
QA/QC	Quality Assurance/Quality Control
R&D	Research and Development
RMF	Risk Management Framework
SAFECode	Software Assurance Forum for Excellence in Code
SCRM	Supply Chain Risk Management
SDLC	System Development Life cycle
SLA	Service-Level Agreement
SOA	Service-Oriented Architecture
SP	Special Publication
U.S.	United States (of America)
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

APPENDIX C

REFERENCES

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

American National Standards Institute/ North American Security Products Organization, ANSI/NASPO-SA-2008.

The Common Criteria Evaluation and Validation Scheme, *Home Page 2008*, URL: http://www.niap-ccevs.org/cc-scheme/, accessed December 5, 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, accessed November 7, 2011.

Department of Homeland Security (DHS), *Sensitive Systems Policy Directive 4300A*, Version 8.0, March 14, 2011, URL: http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf .

Department of Defense (DoD) Manual 5220.22 M, National Industrial Security Program Operating Manual (NISPOM), March 2013.

Homeland Security System Engineering and Development Institute, Information Communication Technology (ICT) Supply Chain Exploit Frame of Reference, March 2013.

International Organization for Standardization/International Organization for Standardization (ISO/IEC) 15288:2008, *Systems and Software Engineering – System Life Cycle Processes*, URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43564, accessed July 2, 2013.

ISO/IEC 12207, *Systems and software engineering – Software life cycle processes.*

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements.*

ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security controls.*

Draft ISO/IEC 27036, Information Technology – Security Techniques – Information Security for Supplier Relationships, April 2013.

ISO 28000:2007, *Specification for Security management systems for the supply chain*, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44641, accessed July 2, 2013.

ISO 9001:2008, *Quality management systems: Requirements*, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46486, accessed July 2, 2013.

National Defense University (NDU), *Software Assurance in Acquisition: Mitigating Risks to the Enterprise*, October 2008, URL: https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf, accessed December 5, 2011.

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

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

National Institute of Standards and Technology, Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.

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 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.

National Institute of Standards and Technology, Special Publication 800-53, Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems*, April 2013.

National Institute of Standards and Technology, Special Publication NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*

NIST Interagency Report (IR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012. http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf .

The Open Group, Open Trusted Technology Provider Standard (O-TTPS) Version 1, *Mitigating Tainted and Counterfeit Products*, April 2013.

Software Assurance Forum for Excellence in Code (SAFECode), *The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain,* July 21, 2009.

SAFECode, Software Integrity Controls, *An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain,* June 14, 2010.

APPENDIX D

NIST SP 800-53 ICT SCRM-RELEVANT CONTROLS

This appendix provides a list of information security controls from NIST Special Publication 800-53rev4 that are directly relevant and apply to supply chain security. The list is categorized alphabetically by existing information security control families. The specific controls within those families are ordered numerically. Note: Control families Program Management (PM) and Planning (PL) are listed separately, as they are considered an oversight activity and ordered as such in NIST SP 800-53rev 4. The controls in this document are linked to the Chapter 3 supply chain risk management (SCRM) guidance to provide an expanded description and frame of reference to the SCRM guidance.

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy [*Assignment: organization-defined frequency*]; and

   2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT [Back to SCRM Control]

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

g. Monitors the use of, information system accounts;

h. Notifies account managers:

1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4) (5) (12) (13)

AC-3 ACCESS ENFORCEMENT [Back to SCRM Control]

Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

AC-3 (8) access enforcement | revocation of access authorizations [Back to SCRM Control]

The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [*Assignment: organization-defined rules governing the timing of revocations of access authorizations*].

Supplemental Guidance: Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-3	**MOD** AC-3	**HIGH** AC-3

AC-4 INFORMATION FLOW ENFORCEMENT *[Back to SCRM Control]*

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.
Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements:

AC-4(6) information flow enforcement | metadata *[Back to SCRM Control]*

The information system enforces information flow control based on [*Assignment: organization-defined metadata*].

Supplemental Guidance: Metadata is information used to describe the characteristics of data. Metadata can include structural metadata describing data structures (e.g., data format, syntax, and semantics) or descriptive metadata describing data contents (e.g., age, location, telephone number). Enforcing allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata with regard to data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., ensuring sufficiently strong binding techniques with appropriate levels of assurance). Related controls: AC-16, SI-7.

AC-4 (17) information flow enforcement | domain authentication *[Back to SCRM Control]*

The information system uniquely identifies and authenticates source and destination points by [*Selection (one or more): organization, system, application, individual*] for information transfer.

Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in information systems, allows the forensic reconstruction of events when required, and encourages policy compliance by attributing policy violations to specific organizations/individuals. Successful domain authentication requires that information system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Related controls: IA-2, IA-3, IA-4, IA-5.

AC-4 (19) information flow enforcement | domain authentication

[Back to SCRM Control]

The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.

Supplemental Guidance: This control enhancement requires the validation of metadata and the data to which the metadata applies. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions, considering metadata and the data to which the metadata applies as part of the payload. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.

AC-4 (21) information flow enforcement | physical / logical separation of information flows *[Back to SCRM Control]*

The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.

References: Web: ucdmo.gov.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES *[Back to SCRM Control]*

Control: The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE [Back to SCRM Control]

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2) (5) (9) (10)	**HIGH** AC-6 (1) (2) (3) (5) (9) (10)

AC-17 REMOTE ACCESS [Back to SCRM Control]

Control: The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

Supplemental Guidance: Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

Control Enhancements:

AC-17(6) remote access | protection of information [Back to SCRM Control]

The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

Supplemental Guidance: Related controls: AT-2, AT-3, PS-6.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	**LOW** AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

AC-18 WIRELESS ACCESS [Back to SCRM Control]

Control: The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. Authorizes wireless access to the information system prior to allowing such connections.

Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

References: NIST Special Publications 800-48, 800-94, 800-97.

Priority and Baseline Allocation:

P1	**LOW** AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (4) (5)

AC-19 ACCESS CONTROL FOR MOBILE DEVICES [Back to SCRM Control]

Control: The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. Authorizes the connection of mobile devices to organizational information systems.

Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

Priority and Baseline Allocation:

P1	**LOW** AC-19	**MOD** AC-19 (5)	**HIGH** AC-19 (5)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS [Back to SCRM Control]

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and

b. Process, store, or transmit organization-controlled information using external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

Control Enhancements:

AC-20(1) use of external information systems | limits on authorized use
[Back to SCRM Control]

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

AC-20(3) use of external information systems | non-organizationally owned systems / components / devices [Back to SCRM Control]

The organization [*Selection: restricts; prohibits*] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

Supplemental Guidance: Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** AC-20	**MOD** AC-20 (1) (2)	**HIGH** AC-20 (1) (2)

AC-21 INFORMATION SHARING [Back to SCRM Control]

Control: The organization:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

b. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

Supplemental Guidance: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AC-21	**HIGH** AC-21

AC-22 PUBLICLY ACCESSIBLE CONTENT [Back to SCRM Control]

Control: The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.

Supplemental Guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AC-22	**MOD** AC-22	**HIGH** AC-22

AC-24 ACCESS CONTROL DECISIONS [Back to SCRM Control]

Control: The organization establishes procedures to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.

Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AWARENESS AND TRAINING

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. Reviews and updates the current:

1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and

2. Security awareness and training procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AT-1	**MOD** AT-1	**HIGH** AT-1

AT-3 Security Training [Back to SCRM Control]

AT-3 (2) security training | physical security controls [Back to SCRM Control]

The organization provides [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training. Related controls: PE-2, PE-3, PE-4, PE-5.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-3	**MOD** AT-3	**HIGH** AT-3

FAMILY: AUDIT AND ACCOUNTABILITY

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:

1. Audit and accountability policy [*Assignment: organization-defined frequency*]; and

2. Audit and accountability procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDIT EVENTS [Back to SCRM Control]

Control: The organization:

a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

Supplemental Guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are *audited* at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

References: NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (3)

AU-3 CONTENT OF AUDIT RECORDS [Back to SCRM Control]

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING [Back to SCRM Control]

Control: The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

b. Reports findings to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

AU-6(6) audit review, analysis, and reporting | correlation with physical monitoring [Back to SCRM Control]

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Supplemental Guidance: The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identify for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.

AU-6 (9) audit review, analysis, and reporting | correlation with information from nontechnical sources [Back to SCRM Control]

The organization correlates information from nontechnical sources with audit information to enhance organization-wide situational awareness.

Supplemental Guidance: Nontechnical sources include, for example, human resources records documenting organizational policy violations (e.g., sexual harassment incidents, improper use of organizational information assets). Such information can lead organizations to a more directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions. Related control: AT-2.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-6	**MOD** AU-6 (1) (3)	**HIGH** AU-6 (1) (3) (5) (6)

AU-10 NON-REPUDIATION [Back to SCRM Control]

Control Enhancements:

AU-10 (1) non-repudiation | association of identities [Back to SCRM Control]

The information system:

(c) **Binds the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and**

(d) **Provides the means for authorized individuals to determine the identity of the producer of the information.**

Supplemental Guidance: This control enhancement supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of the binding between the information producer and the information based on the security category of the information and relevant risk factors. Related controls: AC-4, AC-16.

AU-10 (2) non-repudiation | validate binding of information producer identity [Back to SCRM Control]

The information system:

(a) **Validates the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and**

(b) **Performs [*Assignment: organization-defined actions*] in the event of a validation error.**

Supplemental Guidance: This control enhancement prevents the modification of information between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically. Related controls: AC-3, AC-4, AC-16.

AU-10 (3) non-repudiation | chain of custody [Back to SCRM Control]

The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

Supplemental Guidance: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed. Related controls: AC-4, AC-16.

AU-10 (4) non-repudiation | *validate binding of information reviewer identity*
[Back to SCRM Control]

The information system:

(a) **Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [*Assignment: organization-defined security domains*]; and**

(b) **Performs [*Assignment: organization-defined actions*] in the event of a validation error.**

Supplemental Guidance: This control enhancement prevents the modification of information between review and transfer/release. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine validations are in response to user requests or generated automatically. Related controls: AC-4, AC-16.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AU-10

AU-13 MONITORING FOR INFORMATION DISCLOSURE *[Back to SCRM Control]*

Control: The organization monitors [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information.

Supplemental Guidance: Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-16 CROSS-ORGANIZATIONAL AUDITING [Back to SCRM Control]

Control: The organization employs [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.

Supplemental Guidance: When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:

1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and

2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS [Back to SCRM Control]

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

1. Security controls and control enhancements under assessment;

2. Assessment procedures to be used to determine security control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*].

Supplemental Guidance: Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

Control Enhancements:

CA-2 (2) security assessments | specialized assessments

[Back to SCRM Control]

The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing;* [*Assignment: organization-defined other forms of security assessment*]].

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.

CA-2 (3) security assessments | external organizations [Back to SCRM Control]

The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*Assignment: organization-defined external organization*] when the assessment meets [*Assignment: organization-defined requirements*].

Supplemental Guidance: Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives.

References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137.

Priority and Baseline Allocation:

P2	**LOW** CA-2	**MOD** CA-2 (1)	**HIGH** CA-2 (1) (2)

CA-3 SYSTEM INTERCONNECTIONS [Back to SCRM Control]

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Control Enhancements:

CA-3 (3) system interconnections | unclassified non-national security system connections [Back to SCRM Control]

The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*Assignment; organization-defined boundary protection device*].

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified non-national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).

CA-3 (4) system interconnections | connections to public networks [Back to SCRM Control]

The organization prohibits the direct connection of an [*Assignment: organization-defined information system*] to a public network.

Supplemental Guidance: A public network is any network accessible to the general public including, for example, the Internet and organizational extranets with public access.

CA-3 (5) system interconnections | restrictions on external system connections [Back to SCRM Control]

The organization employs [*Selection: allow-all, deny-by-exception; deny-all, permit-by-exception*] policy for allowing [*Assignment: organization-defined information systems*] to connect to external information systems.

Supplemental Guidance: Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as *blacklisting* (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as *whitelisting* (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.

References: FIPS Publication 199; NIST Special Publication 800-47.

Priority and Baseline Allocation:

P1	**LOW** CA-3	**MOD** CA-3 (5)	**HIGH** CA-3 (5)

CA-5 PLAN OF ACTION AND MILESTONES [Back to SCRM Control]

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	**LOW** CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY AUTHORIZATION [Back to SCRM Control]

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization [*Assignment: organization-defined frequency*].

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements: None.

References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137.

Priority and Baseline Allocation:

P2	**LOW** CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control Enhancements:

CA-7 (3) continuous monitoring | trend analyses [Back to SCRM Control]

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.

References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

Priority and Baseline Allocation:

P2	**LOW** CA-7	**MOD** CA-7 (1)	**HIGH** CA-7 (1)

FAMILY: CONFIGURATION MANAGEMENT

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

1. Configuration management policy [*Assignment: organization-defined frequency*]; and

2. Configuration management procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION [Back to SCRM Control]

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

Control Enhancements:

CM-2 (1) baseline configuration | *reviews and updates* [Back to SCRM Control]

The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

CM-2 (6) baseline configuration | *development and test environments* [Back to SCRM Control]

The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4, SC-3, SC-7.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-2	**MOD** CM-2 (1) (3) (7)	**HIGH** CM-2 (1) (2) (3) (7)

CM-3 CONFIGURATION CHANGE CONTROL [Back to SCRM Control]

Control: The organization:

a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

e. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Supplemental Guidance: Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

Control Enhancements:

CM-3 (1) configuration change control | automated document / notification / prohibition of changes [Back to SCRM Control]

The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [*Assignment: organized-defined approval authorities*] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [*Assignment: organization-defined time period*];

(d) Prohibit changes to the information system until designated approvals are received;

(e) Document all changes to the information system; and

(f) Notify [*Assignment: organization-defined personnel*] when approved changes to the information system are completed.

CM-3 (2) configuration change control | test / validate / document changes [Back to SCRM Control]

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-3 (2)	**HIGH** CM-3 (1) (2)

CM-4 SECURITY IMPACT ANALYSIS *[Back to SCRM Control]*

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Control Enhancements:

CM-4 (1) security impact analysis | separate test environments *[Back to SCRM Control]*

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P2	**LOW** CM-4	**MOD** CM-4	**HIGH** CM-4 (1)

CM-5 ACCESS RESTRICTIONS FOR CHANGE *[Back to SCRM Control]*

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

CM-5 (1) access restrictions for change | automated access enforcement / auditing [Back to SCRM Control]

The information system enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

CM-5 (2) access restrictions for change | review system changes [Back to SCRM Control]

The organization reviews information system changes [*Assignment: organization-defined frequency*] and [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.

Supplemental Guidance: Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

CM-5 (3) access restrictions for change | signed components [Back to SCRM Control]

The information system prevents the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.

CM-5 (6) access restrictions for change | limit library privileges [Back to SCRM Control]

The organization limits privileges to change software resident within software libraries.

Supplemental Guidance: Software libraries include privileged programs. Related control: AC-2.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-5	**HIGH** CM-5 (1) (2) (3)

CM-6 CONFIGURATION SETTINGS [Back to SCRM Control]

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

Control Enhancements:

CM-6 (1) configuration settings | automated central management / application / verification   [Back to SCRM Control]

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

Supplemental Guidance: Related controls: CA-7, CM-4.

CM-6 (2) configuration settings | respond to unauthorized changes [Back to SCRM Control]

The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7.

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov.

Priority and Baseline Allocation:

P1	**LOW** CM-6	**MOD** CM-6	**HIGH** CM-6 (1) (2)

CM-7 LEAST FUNCTIONALITY [Back to SCRM Control]

Control: The organization:

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.

Control Enhancements:

CM-7 (1) least functionality | periodic review [Back to SCRM Control]

The organization:

(g) **Reviews the information system [*Assignment: organization-defined frequency*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and**

(h) **Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].**

Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.

CM-7 (4) least functionality | *unauthorized software / blacklisting* [Back to SCRM Control]

The organization:

(a) Identifies [*Assignment: organization-defined software programs not authorized to execute on the information system*];

(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs [*Assignment: organization-defined frequency*].

Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as *blacklisting*. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.

CM-7 (5) least functionality | *authorized software / whitelisting* [Back to SCRM Control]

The organization:

(a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];

(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

(c) Reviews and updates the list of authorized software programs [*Assignment: organization-defined frequency*].

Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as *whitelisting*. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

References: DoD Instruction 8551.01.

Priority and Baseline Allocation:

P1	**LOW** CM-7	**MOD** CM-7 (1) (2) (4)	**HIGH** CM-7 (1) (2) (5)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY [Back to SCRM Control]

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;

2. Includes all components within the authorization boundary of the information system;

3. Is at the level of granularity deemed necessary for tracking and reporting; and

4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.

Control Enhancements:

CM-8 (1) information system component inventory | updates during installations / removals [Back to SCRM Control]

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

CM-8 (2) information system component inventory | automated maintenance [Back to SCRM Control]

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Supplemental Guidance: Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related control: SI-7.

CM-8 (4) information system component inventory | accountability information [Back to SCRM Control]

The organization includes in the information system component inventory information, a means for identifying by [*Selection (one or more): name; position; role*], individuals responsible/accountable for administering those components.

Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach/compromise, component needs to be recalled/replaced, or component needs to be relocated).

CM-8 (6) information system component inventory | assessed configurations / approved deviations [Back to SCRM Control]

The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Supplemental Guidance: This control enhancement focuses on configuration settings established by organizations for information system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings. Related controls: CM-2, CM-6.

CM-8 (7) information system component inventory | centralized repository [Back to SCRM Control]

The organization provides a centralized repository for the inventory of information system components.

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. Centralized repositories of information system component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner).

CM-8 (8) information system component inventory | automated location tracking [Back to SCRM Control]

The organization employs automated mechanisms to support tracking of information system components by geographic location.

Supplemental Guidance: The use of automated mechanisms to track the location of information system components can increase the accuracy of component inventories. Such capability may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions.

CM-8 (9) information system component inventory | assignment of components to systems [Back to SCRM Control]

The organization:

(a) Assigns [*Assignment: organization-defined acquired information system components*] to an information system; and

(b) Receives an acknowledgement from the information system owner of this assignment.

Supplemental Guidance: Organizations determine the criteria for or types of information system components (e.g., microprocessors, motherboards, software, programmable logic controllers, and network devices) that are subject to this control enhancement. Related control: SA-4.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-8	**MOD** CM-8 (1) (3) (5)	**HIGH** CM-8 (1) (2) (3) (4) (5)

CM-9 CONFIGURATION MANAGEMENT PLAN *[Back to SCRM Control]*

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the information system and places the configuration items under configuration management; and

d. Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Control Enhancements:

CM-9 (1) configuration management plan | assignment of responsibility *[Back to SCRM Control]*

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.

Supplemental Guidance: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the information system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CM-9	HIGH CM-9

CM-10 SOFTWARE USAGE RESTRICTIONS [Back to SCRM Control]

Control: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.

Control Enhancements:

CM-10 (1) software usage restrictions | open source software [Back to SCRM Control]

The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

Supplemental Guidance: Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

References: None.

Priority and Baseline Allocation:

P2	LOW CM-10	MOD CM-10	HIGH CM-10

CM-11 USER-INSTALLED SOFTWARE [Back to SCRM Control]

Control: The organization:

a. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;

b. Enforces software installation policies through [*Assignment: organization-defined methods*]; and

c. Monitors policy compliance at [*Assignment: organization-defined frequency*].

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation.

Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

References: None.

Priority and Baseline Allocation:

P1	**LOW** CM-11	**MOD** CM-11	**HIGH** CM-11

FAMILY: CONTINGENCY PLANNING

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES
[Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:

   1. Contingency planning policy [*Assignment: organization-defined frequency*]; and

   2. Contingency planning procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN *[Back to SCRM Control]*

Control: The organization:

a. Develops a contingency plan for the information system that:

   1. Identifies essential missions and business functions and associated contingency requirements;

   2. Provides recovery objectives, restoration priorities, and metrics;

   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

Control Enhancements:

CP-2 (7) contingency plan | coordinate with external service providers [Back to SCRM Control]

The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9.

CP-2 (8) contingency plan | identify critical assets [Back to SCRM Control]

The organization identifies critical information system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-2	**MOD** CP-2 (1) (3) (8)	**HIGH** CP-2 (1) (2) (3) (4) (5) (8)

CP-6 ALTERNATE STORAGE SITE *[Back to SCRM Control]*

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE [Back to SCRM Control]

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-7 (1) (2) (3)	**HIGH** CP-7 (1) (2) (3) (4)

CP-8 TELECOMMUNICATIONS SERVICES [Back to SCRM Control]

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.

Control Enhancements:

CP-8 (3) telecommunications services | separation of primary / alternate providers [Back to SCRM Control]

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

CP-8 (4) telecommunications services | provider contingency plan

[Back to SCRM Control]

The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtains evidence of contingency testing/training by providers [*Assignment: organization-defined frequency*].

Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

FAMILY: IDENTIFICATION AND AUTHENTICATION

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

   1. Identification and authentication policy [*Assignment: organization-defined frequency*]; and

   2. Identification and authentication procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) *[Back to SCRM Control]*

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-2 (1) (12)	**MOD** IA-2 (1) (2) (3) (8) (11) (12)	**HIGH** IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

IA-4 IDENTIFIER MANAGEMENT *[Back to SCRM Control]*

Control: The organization manages information system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device;

d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*]; and

e. Disabling the identifier after [*Assignment: organization-defined time period of inactivity*].

Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Control Enhancements:

IA-4 (4) identifier management | identify user status [Back to SCRM Control]

The organization manages individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor. Related control: AT-2.

IA-4 (5) identifier management | dynamic management
[Back to SCRM Control]

The information system dynamically manages identifiers.

Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed information systems including, for example, service-oriented architectures, rely on establishing identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential. Related control: AC-16.

IA-4 (6) identifier management | cross-organization management
[Back to SCRM Control]

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of identifiers.

Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT [Back to SCRM Control]

Control: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Control Enhancements:

IA-5 (5) authenticator management | change authenticators prior to delivery [Back to SCRM Control]

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

IA-5 (9) authenticator management | cross-organization credential management [Back to SCRM Control]

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of credentials.

Supplemental Guidance: Cross-organization management of credentials provides the capability for organizations to appropriately authenticate individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-5 (1) (11)	**MOD** IA-5 (1) (2) (3) (11)	**HIGH** IA-5 (1) (2) (3) (11)

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) [Back to SCRM Control]

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-8 (1) (2) (3) (4)	**MOD** IA-8 (1) (2) (3) (4)	**HIGH** IA-8 (1) (2) (3) (4)

FAMILY: INCIDENT RESPONSE

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES   *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

1. Incident response policy [*Assignment: organization-defined frequency*]; and

2. Incident response procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IR-1	**MOD** IR-1	**HIGH** IR-1

IR-4 INCIDENT HANDLING *[Back to SCRM Control]*

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

IR-4 (10) incident handling | supply chain coordination *[Back to SCRM Control]*

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

References: Executive Order 13587; NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1) (4)

IR-6 INCIDENT REPORTING *[Back to SCRM Control]*

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and

b. Reports security incident information to [*Assignment: organization-defined authorities*].

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.

Control Enhancements:

IR-6 (3) incident reporting | coordination with supply chain [Back to SCRM Control]

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to sensitive information being released to outside organizations of perhaps questionable trustworthiness.

References: NIST Special Publication 800-61: Web: www.us-cert.gov.

Priority and Baseline Allocation:

P1	**LOW** IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-9 INFORMATION SPILLAGE RESPONSE [Back to SCRM Control]

Control: The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

c. Isolating the contaminated information system or system component;

d. Eradicating the information from the contaminated information system or component;

e. Identifying other information systems or system components that may have been subsequently contaminated; and

f. Performing other [*Assignment: organization-defined actions*].

Supplemental Guidance: Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: MAINTENANCE

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES [*[Back to SCRM Control]*]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

   1. System maintenance policy [*Assignment: organization-defined frequency*]; and

   2. System maintenance procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control Enhancements:

MA-2 (2) controlled maintenance | automated maintenance activities *[Back to SCRM Control]*

The organization:

(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Supplemental Guidance: Related controls: CA-7, MA-3.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-2	**MOD** MA-2	**HIGH** MA-2 (2)

MA-3 MAINTENANCE TOOLS [Back to SCRM Control]

Control: The organization approves, controls, and monitors information system maintenance tools.

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.

Control Enhancements:

MA-3 (1) maintenance tools | inspect tools [Back to SCRM Control]

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.

MA-3 (2) maintenance tools | inspect media [Back to SCRM Control]

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.

MA-3 (3) maintenance tools | prevent unauthorized removal [Back to SCRM Control]

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [*Assignment: organization-defined personnel or roles*] explicitly authorizing removal of the equipment from the facility.

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

References: NIST Special Publication 800-88.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** MA-3 (1) (2)	**HIGH** MA-3 (1) (2) (3)

MA-4 NONLOCAL MAINTENANCE [Back to SCRM Control]

Control: The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;

b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.

Control Enhancements:

MA-4 (2) nonlocal maintenance | document nonlocal maintenance [Back to SCRM Control]

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

MA-4 (3) nonlocal maintenance | comparable security / sanitization [Back to SCRM Control]

The organization:

(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to

potentially malicious software) before reconnecting the component to the information system.

Supplemental Guidance: Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7.

MA-4 (5) nonlocal maintenance | *approvals and notifications* [Back to SCRM Control]

The organization:

(a) **Requires the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and**

(b) **Notifies [*Assignment: organization-defined personnel or roles*] of the date and time of planned nonlocal maintenance.**

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and information system knowledge to determine the appropriateness of the proposed maintenance.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

P2	**LOW** MA-4	**MOD** MA-4 (2)	**HIGH** MA-4 (2) (3)

MA-5 MAINTENANCE PERSONNEL *[Back to SCRM Control]*

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-5	**MOD** MA-5	**HIGH** MA-5 (1)

MA-6 TIMELY MAINTENANCE [Back to SCRM Control]

Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** MA-6	**HIGH** MA-6

FAMILY: MEDIA PROTECTION

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:

1. Media protection policy [*Assignment: organization-defined frequency*]; and

2. Media protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** MP-1	**MOD** MP-1	**HIGH** MP-1

MP-5 MEDIA TRANSPORT *[Back to SCRM Control]*

Control: The organization:

a. Protects and controls [*Assignment: organization-defined types of information system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*];

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

References: FIPS Publication 199; NIST Special Publication 800-60.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-5 (4)	**HIGH** MP-5 (4)

MP-6 MEDIA SANITIZATION [Back to SCRM Control]

Control: The organization:

a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

Control Enhancements:

MP-6 (1) media sanitization | review / approve / track / document / verify [Back to SCRM Control]

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental Guidance: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.

MP-6 (2) media sanitization | equipment testing [Back to SCRM Control]

The organization tests sanitization equipment and procedures [*Assignment: organization-defined frequency*] to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

MP-6 (3) media sanitization | nondestructive techniques [Back to SCRM Control]

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

Supplemental Guidance: This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

MP-6 (7) media sanitization | dual authorization [Back to SCRM Control]

The organization enforces dual authorization for the sanitization of [*Assignment: organization-defined information system media*].

Supplemental Guidance: Organizations employ dual authorization to ensure that information system media sanitization cannot occur unless two technically qualified individuals conduct the task. Individuals sanitizing information system media possess sufficient skills/expertise to determine if the proposed sanitization reflects applicable federal/organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, both protecting against errors and false claims of having performed the sanitization actions. Related controls: AC-3, MP-2.

MP-6 (8) media sanitization | remote purging / wiping of information [Back to SCRM Control]

The organization provides the capability to purge/wipe information from [*Assignment: organization-defined information systems, system components, or devices*] either remotely or under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: This control enhancement protects data/information on organizational information systems, system components, or devices (e.g., mobile devices) if such systems, components, or devices are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge/wipe function can be implemented in a variety of ways including, for example, by overwriting data/information multiple times or by destroying the key necessary to decrypt encrypted data.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

Priority and Baseline Allocation:

P1	**LOW** MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2) (3)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. Reviews and updates the current:

1. Physical and environmental protection policy [*Assignment: organization-defined frequency*]; and

2. Physical and environmental protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PE-1	**MOD** PE-1	**HIGH** PE-1

PE-3 PHYSICAL ACCESS CONTROL *[Back to SCRM Control]*

Control: The organization:

a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress/egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems/devices*]; *guards*];

b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];

e. Secures keys, combinations, and other physical access devices;

f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Control Enhancements:

PE-3 (5) physical access control | tamper protection [Back to SCRM Control]

The organization employs [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the information system.

Supplemental Guidance: Organizations may implement tamper detection/prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Tamper detection/prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks. Related control: SA-12.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov.

Priority and Baseline Allocation:

P1	**LOW** PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-6 MONITORING PHYSICAL ACCESS [Back to SCRM Control]

Control: The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and

c. Coordinates results of reviews and investigations with the organizational incident response capability.

Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (4)

PE-16 DELIVERY AND REMOVAL [Back to SCRM Control]

Control: The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE [Back to SCRM Control]

Control: The organization:

a. Employs [*Assignment: organization-defined security controls*] at alternate work sites;

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative. Related controls: AC-17, CP-7.

Control Enhancements: None.

References: NIST Special Publication 800-46.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS [Back to SCRM Control]

Control: The organization positions information system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.

Control Enhancements:

PE-18 (1) location of information system components | facility site [Back to SCRM Control]

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Supplemental Guidance: Related control: PM-8.

References: None.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** Not Selected	**HIGH** PE-18

PE-19 INFORMATION LEAKAGE [Back to SCRM Control]

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: Information leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Control Enhancements:

(1) *INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*

The organization ensures that information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

PE-20 ASSET MONITORING AND TRACKING [Back to SCRM Control]

Control: The organization:

a. Employs [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*]; and

b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Supplemental Guidance: Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns. Related control: CM-8.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PERSONNEL SECURITY

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:

   1. Personnel security policy [*Assignment: organization-defined frequency*]; and

   2. Personnel security procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PS-1	**MOD** PS-1	**HIGH** PS-1

PS-6 ACCESS AGREEMENTS *[Back to SCRM Control]*

Control: The organization:

a. Develops and documents access agreements for organizational information systems;

b. Reviews and updates the access agreements [*Assignment: organization-defined frequency*]; and

c. Ensures that individuals requiring access to organizational information and information systems:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY [Back to SCRM Control]

Control: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;

c. Documents personnel security requirements;

d. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*Assignment: organization-defined time period*]; and

e. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Control Enhancements: None.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** PS-7	**MOD** PS-7	**HIGH** PS-7

FAMILY: RISK ASSESSMENT

RA-1 *RISK ASSESSMENT POLICY AND PROCEDURES* [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

1. Risk assessment policy [*Assignment: organization-defined frequency*]; and

2. Risk assessment procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.

Priority and Baseline Allocation:

P1	**LOW** RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 *SECURITY CATEGORIZATION* [Back to SCRM Control]

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	**LOW** RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT [Back to SCRM Control]

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];

c. Reviews risk assessment results [*Assignment: organization-defined frequency*];

d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework.

Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.

Control Enhancements: None.

References: OMB Memorandum 04-04; NIST Special Publication 800-30, 800-39; Web: idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** RA-3	**MOD** RA-3	**HIGH** RA-3

FAMILY: SYSTEM AND SERVICES ACQUISITION

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

1. System and services acquisition policy [*Assignment: organization-defined frequency*]; and

2. System and services acquisition procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES *[Back to SCRM Control]*

Control: The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Priority and Baseline Allocation:

P1	**LOW** SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE [Back to SCRM Control]

Control: The organization:

a. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and

d. Integrates the organizational information security risk management process into system development life cycle activities.

Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-64.

Priority and Baseline Allocation:

P1	**LOW** SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITION PROCESS [Back to SCRM Control]

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

Supplemental Guidance: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Control Enhancements:

SA-4 (1) acquisition process | functional properties of security controls [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.

SA-4 (5) acquisition process | system / component / service configurations [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to:

(a) **Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and**

(b) **Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.**

Supplemental Guidance: Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8.

SA-4 (7) acquisition process | niap-approved protection profiles [Back to SCRM Control]

The organization:

(a) **Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and**

(b) **Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.**

Supplemental Guidance: Related controls: SC-12, SC-13.

SA-4 (8) acquisition process | continuous monitoring plan [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*Assignment: organization-defined level of detail*].

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations. Related control: CA-7.

SA-4 (9) acquisition process | functions / ports / protocols / services in use [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.

References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far.

Priority and Baseline Allocation:

P1	**LOW** SA-4 (10)	**MOD** SA-4 (1) (2) (9) (10)	**HIGH** SA-4 (1) (2) (9) (10)

SA-5 INFORMATION SYSTEM DOCUMENTATION [Back to SCRM Control]

Control: The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security functions/mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:

   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

   3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements:

(1) *INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*

[Withdrawn: Incorporated into SA-4 (1)].

(2) *INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*

[Withdrawn: Incorporated into SA-4 (2)].

(3) *INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*

[Withdrawn: Incorporated into SA-4 (2)].

(4) *INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*

[Withdrawn: Incorporated into SA-4 (2)].

(5) *INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*

[Withdrawn: Incorporated into SA-4 (2)].

References: None.

Priority and Baseline Allocation:

P2	**LOW** SA-5	**MOD** SA-5	**HIGH** SA-5

SA-8 SECURITY ENGINEERING PRINCIPLES [Back to SCRM Control]

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES *[Back to SCRM Control]*

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

Supplemental Guidance: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Enhancements:

SA-9 (1) external information systems | risk assessments / organizational approvals *[Back to SCRM Control]*

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) **Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].**

Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3.

SA-9 (3) external information systems | establish / maintain trust relationship with providers [Back to SCRM Control]

The organization establishes, documents, and maintains trust relationships with external service providers based on [*Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. Such relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and the types of interactions between the parties. In some cases, the degree of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls. The level of control is typically established by the terms and conditions of the contracts or service-level agreements and can range from extensive control (e.g., negotiating contracts or agreements that specify security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services). In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.

SA-9 (4) external information systems | consistent interests of consumers and providers [Back to SCRM Control]

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests.

Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.

SA-9 (5) external information systems | processing, storage, and service location [Back to SCRM Control]

> **The organization restricts the location of [*Selection (one or more): information processing; information/data; information system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].**
>
> Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** SA-9	**MOD** SA-9 (2)	**HIGH** SA-9 (2)

SA-10 DEVELOPER CONFIGURATION MANAGEMENT [Back to SCRM Control]

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*];

b. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

Supplemental Guidance: This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.

<u>Control Enhancements:</u>

SA-10 (1) developer configuration management | software / firmware integrity verification *[Back to SCRM Control]*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

<u>Supplemental Guidance</u>: This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components. Related control: SI-7.

SA-10 (2) developer configuration management | alternative configuration management processes *[Back to SCRM Control]*

The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

<u>Supplemental Guidance</u>: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf (COTS) information technology products. Alternate configuration management processes include organizational personnel that: (i) are responsible for reviewing/approving proposed changes to information systems, system components, and information system services; and (ii) conduct security impact analyses prior to the implementation of any changes to systems, components, or services (e.g., a configuration control board that considers security impacts of changes during development and includes representatives of both the organization and the developer, when applicable).

SA-10 (3) developer configuration management | hardware integrity verification *[Back to SCRM Control]*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

<u>Supplemental Guidance</u>: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components. Related control: SI-7.

SA-10 (4) developer configuration management | trusted generation *[Back to SCRM Control]*

The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of

security-relevant hardware descriptions and software/firmware source and object code with previous versions.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components between versions during development. In contrast, SA-10 (1) and SA-10 (3) allow organizations to detect unauthorized changes to hardware, software, and firmware components through the use of tools, techniques, and/or mechanisms provided by developers.

SA-10 (5) developer configuration management | mapping integrity for version control [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational information systems supporting critical missions and/or business functions.

SA-10 (6) developer configuration management | trusted distribution [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that such updates are faithful representations of the master copies maintained by the developer and have not been tampered with during distribution.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-10	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION [Back to SCRM Control]

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;

b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The *depth* of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The *coverage* of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Control Enhancements:

SA-11(1) developer security testing and evaluation | static code analysis

[Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

SA-11(2) developer security testing and evaluation | threat and vulnerability analyses

[Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.

SA-11(3) developer security testing and evaluation | independent verification of assessment plans / evidence *[Back to SCRM Control]*

The organization:

(c) **Requires an independent agent satisfying [*Assignment: organization-defined independence criteria*] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and**

(d) **Ensures that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.**

Supplemental Guidance: Independent agents have the necessary qualifications (i.e., expertise, skills, training, and experience) to verify the correct implementation of developer security assessment plans. Related controls: AT-3, CA-7, RA-5, SA-12.

SA-11(4) developer security testing and evaluation | manual code reviews [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment*: organization-defined specific code*] using [*Assignment: organization-defined processes, procedures, and/or techniques*].

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application’s requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.

SA-11(5) developer security testing and evaluation | penetration testing / analysis [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [*Assignment: organization-defined breadth/depth*] and with [*Assignment: organization-defined constraints*].

Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

SA-11(6) developer security testing and evaluation | attack surface reviews [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

Supplemental Guidance: Attack surfaces of information systems are exposed areas that make those systems more vulnerable to cyber attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.

SA-11(7) developer security testing and evaluation | verify scope of testing / evaluation [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [*Assignment: organization-defined depth of testing/evaluation*].

Supplemental Guidance: Verifying that security testing/evaluation provides complete coverage of required security controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating security control coverage at the highest levels of assurance can be provided by the use of formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.

SA-11(8) developer security testing and evaluation | dynamic code analysis [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications.

References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-11	**HIGH** SA-11

SA-12 SUPPLY CHAIN PROTECTION [Back to SCRM Control]

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

Supplemental Guidance: Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

Control Enhancements:

SA-12 (1) supply chain protection | acquisition strategies / tools / methods [Back to SCRM Control]

The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.

Supplemental Guidance: The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing). Related control: SA-19.

SA-12 (2) supply chain protection | supplier reviews [Back to SCRM Control]

The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.

Supplemental Guidance: Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.

SA-12 (5) supply chain protection | limitation of harm *[Back to SCRM Control]*

The organization employs [*Assignment: organization-defined security safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.

Supplemental Guidance: Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example: (i) avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations; (ii) employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; (iii) employing approved vendor lists with standing reputations in industry, and (iv) using procurement carve outs (i.e., exclusions to commitments or obligations).

SA-12 (7) supply chain protection | assessments prior to selection / acceptance / update *[Back to SCRM Control]*

The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update.

Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, tools, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by organizations. Related controls: CA-2, SA-11.

SA-12 (8) supply chain protection | use of all-source intelligence *[Back to SCRM Control]*

The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.

Supplemental Guidance: All-source intelligence analysis is employed by organizations to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence. Where available, such information is used to analyze the risk of both intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review is performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Related control: SA-15.

SA-12 (9) supply chain protection | operations security *[Back to SCRM Control]*

The organization employs [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

Supplemental Guidance: Supply chain information includes, for example: user identities; uses for information systems, information system components, and information system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system/component configurations. This control enhancement expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to: (i) identify those actions that can be observed by potential adversaries; (ii) determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to organizations; (iii) implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and (iv) consider how aggregated information may compromise the confidentiality of users or uses of the supply chain. OPSEC may require organizations to withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users, of information systems, system components, or information system services. Related control: PE-21.

SA-12 (10) supply chain protection | validate as genuine and not altered [Back to SCRM Control]

The organization employs [*Assignment: organization-defined security safeguards*] to validate that the information system or system component received is genuine and has not been altered.

Supplemental Guidance: For some information system components, especially hardware, there are technical means to help determine if the components are genuine or have been altered. Security safeguards used to validate the authenticity of information systems and information system components include, for example, optical/nanotechnology tagging and side-channel analysis. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component and production location.

SA-12 (11) supply chain protection | penetration testing / analysis of elements, processes, and actors [Back to SCRM Control]

The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *information system, system component, or information system service*.

Supplemental Guidance: This control enhancement addresses analysis and/or testing of the supply chain, not just delivered items. Supply chain elements are information technology products or product components that contain programmable logic and that are critically important to information system functions. Supply chain processes include, for example: (i) hardware, software, and firmware development processes; (ii) shipping/handling procedures; (iii) personnel and physical security programs; (iv) configuration management tools/measures to maintain provenance; or (v) any other programs, processes, or procedures associated with the production/distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions. Related control: RA-5.

SA-12 (12) supply chain protection | inter-organizational agreements [Back to SCRM Control]

The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service.

Supplemental Guidance: The establishment of inter-organizational agreements and procedures provides for notification of supply chain compromises. Early notification of supply chain compromises that can potentially adversely affect or have adversely affected organizational information systems, including critical system components, is essential for organizations to provide appropriate responses to such incidents.

SA-12 (13) supply chain protection | critical information system components [Back to SCRM Control]

The organization employs [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Adversaries can attempt to impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations. Safeguards to ensure adequate supplies of critical information system components include, for example: (i) the use of multiple suppliers throughout the supply chain for the identified critical components; and (ii) stockpiling of spare components to ensure operation during mission-critical times.

SA-12 (14) supply chain protection | identity and traceability [Back to SCRM Control]

The organization establishes and retains unique identification of [*Assignment: organization-defined supply chain elements, processes, and actors*] for the information system, system component, or information system service.

Supplemental Guidance: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into what is happening within such supply chains, as well as monitoring and identifying high-risk events and activities. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and actors), it is very difficult for organizations to understand and therefore manage risk, and to reduce the likelihood of adverse events. Uniquely identifying acquirer and integrator roles, organizations, personnel, mission and element processes, testing and evaluation procedures, delivery mechanisms, support mechanisms, communications/delivery paths, and disposal/final disposition activities as well as the components and tools used, establishes a foundational identity structure for assessment of supply chain activities. For example, labeling (using serial numbers) and tagging (using radio-frequency identification [RFID] tags) individual supply chain elements including software packages, modules, and hardware devices, and processes associated with those elements can be used for this purpose. Identification methods are sufficient to support the provenance in the event of a supply chain issue or adverse supply chain event.

SA-12 (15) supply chain protection | processes to address weaknesses or deficiencies [Back to SCRM Control]

The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

Supplemental Guidance: Evidence generated during independent or organizational assessments of supply chain elements (e.g., penetration testing, audits, verification/validation activities) is documented and used in follow-on processes implemented by organizations to respond to the risks related to the identified weaknesses and deficiencies. Supply chain elements include, for example, supplier development processes and supplier distribution systems.

References: NIST Special Publication 800-161; NIST Interagency Report 7622.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-12

SA-14 CRITICALITY ANALYSIS [Back to SCRM Control]

Control: The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

Control Enhancements: None.

(1) *CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*

[Withdrawn: Incorporated into SA-20].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS [Back to SCRM Control]

Control: The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:

1. Explicitly addresses security requirements;

2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and

4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations [*Assignment: organization-defined frequency*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*Assignment: organization-defined security requirements*].

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements:

SA-15 (1) development process, standards, and tools | quality metrics [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to:

(a) Define quality metrics at the beginning of the development process; and

(b) Provide evidence of meeting the quality metrics [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined program review milestones*]; *upon delivery*].

Supplemental Guidance: Organizations use quality metrics to establish minimum acceptable levels of information system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of particular phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or an explicit determination that the warnings have no impact on the effectiveness of required security capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. These metrics can include defining the severity thresholds of vulnerabilities, for example, requiring no known vulnerabilities in the delivered information system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.

SA-15 (2) development process, standards, and tools | security tracking tools [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

Supplemental Guidance: Information system development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes.

SA-15 (3) development process, standards, and tools | criticality analysis [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth*] and at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by organizations in SA-14. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for information system components that are developed as commercial off-the-shelf (COTS) information technology products (e.g., functional specifications, high-level designs, low-level designs, and source code/hardware schematics). Related controls: SA-4, SA-14.

SA-15 (4) development process, standards, and tools | threat modeling / vulnerability analysis [Back to SCRM Control]

The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that:

(a) Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*];

(b) Employs [*Assignment: organization-defined tools and methods*]; and

(c) Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].

Supplemental Guidance: Related control: SA-4.

SA-15 (5) development process, standards, and tools | attack surface reduction [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].

Supplemental Guidance: Attack surface reduction is closely aligned with developer threat and vulnerability analyses and information system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within information systems, information system components, and information system services. Attack surface reduction includes, for example, applying the principle of least privilege, employing layered defenses, applying the principle of least functionality (i.e., restricting ports, protocols, functions, and services), deprecating unsafe functions, and eliminating application programming interfaces (APIs) that are vulnerable to cyber attacks. Related control: CM-7.

SA-15 (6) development process, standards, and tools | continuous improvement [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

Supplemental Guidance: Developers of information systems, information system components, and information system services consider the effectiveness/efficiency of current development processes for meeting quality objectives and addressing security capabilities in current threat environments.

SA-15 (7) development process, standards, and tools | automated vulnerability analysis [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to:

(a) Perform an automated vulnerability analysis using [*Assignment: organization-defined tools*];

(b) Determine the exploitation potential for discovered vulnerabilities;

(c) Determine potential risk mitigations for delivered vulnerabilities; and

(d) Deliver the outputs of the tools and results of the analysis to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related control: RA-5.

SA-15 (8) development process, standards, and tools | reuse of threat / vulnerability information [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Supplemental Guidance: Analysis of vulnerabilities found in similar software applications can inform potential design or implementation issues for information systems under development. Similar information systems or system components may exist within developer organizations. Authoritative vulnerability information is available from a variety of public and private sector sources including, for example, the National Vulnerability Database.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-15

SA-16 DEVELOPER-PROVIDED TRAINING [Back to SCRM Control]

Control: The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.

Control Enhancements:

SA-16 (1) transmission of security attributes | integrity validation [Back to SCRM Control]

The information system validates the integrity of transmitted security attributes.

Supplemental Guidance: This control enhancement ensures that the verification of the integrity of transmitted information includes security attributes. Related controls: AU-10, SC-8.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-16

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control Enhancements:

SA-17 (1) developer security architecture and design | formal policy model *[Back to SCRM Control]*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal policy model describing the [*Assignment: organization-defined elements of organizational security policy*] to be enforced; and

(b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

Supplemental Guidance: Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors/policies to be formally proven. Not all components of information systems can be modeled, and generally, formal specifications are scoped to specific behaviors or policies of interest (e.g., nondiscretionary access control policies). Organizations choose the particular formal modeling language and approach based on the nature of the behaviors/policies to be described and the available tools. Formal modeling tools include, for example, Gypsy and Zed.

SA-17 (3) developer security architecture and design | formal correspondence *[Back to SCRM Control]*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are satisfied by the formal information system description, and that the formal system description is correctly implemented by a description of some lower level, for example a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal/informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input/output. Related control: SA-5.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-17

SA-18 TAMPER RESISTANCE AND DETECTION *[Back to SCRM Control]*

Control: The organization implements a tamper protection program for the information system, system component, or information system service.

Supplemental Guidance: Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

SA-18 (1) tamper resistance and detection | multiple phases of sdlc *[Back to SCRM Control]*

The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage. Related control: SA-3.

SA-18 (2) tamper resistance and detection | inspection of information systems, components, or devices *[Back to SCRM Control]*

The organization inspects [*Assignment: organization-defined information systems, system components, or devices*] [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.

Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of need for inspection include, for example, when individuals return from travel to high-risk locations. Related control: SI-4.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-19 COMPONENT AUTHENTICITY *[Back to SCRM Control]*

Control: The organization:

a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and

b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]; [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

SA-19 (1) component authenticity | anti-counterfeit training *[Back to SCRM Control]*

The organization trains [*Assignment: organization-defined personnel or roles*] to detect counterfeit information system components (including hardware, software, and firmware).

SA-19 (2) component authenticity | configuration control for component service / repair *[Back to SCRM Control]*

The organization maintains configuration control over [*Assignment: organization-defined information system components*] awaiting service/repair and serviced/repaired components awaiting return to service.

SA-19 (3) component authenticity | component disposal *[Back to SCRM Control]*

The organization disposes of information system components using [*Assignment: organization-defined techniques and methods*].

Supplemental Guidance: Proper disposal of information system components helps to prevent such components from entering the gray market.

SA-19 (4) component authenticity | anti-counterfeit training *[Back to SCRM Control]*

The organization scans for counterfeit information system components [*Assignment: organization-defined frequency*].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS *[Back to SCRM Control]*

Control: The organization re-implements or custom develops [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Organizations determine that certain information system components likely cannot be trusted due to specific threats to and vulnerabilities in those components, and for which there are no viable security controls to adequately mitigate the resulting risk. Re-implementation or custom development of such components helps to satisfy requirements for higher assurance. This is accomplished by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to re-implement or custom develop critical information system components, additional safeguards can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files. Related controls: CP-2, SA-8, SA-14.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-21 DEVELOPER SCREENING *[Back to SCRM Control]*

Control: The organization requires that the developer of [*Assignment: organization-defined information system, system component, or information system service*]:

a. Have appropriate access authorizations as determined by assigned [*Assignment: organization-defined official government duties*]; and

b. Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed. Related controls: PS-3, PS-7.

Control Enhancements:

SA-21 (1) developer screening | validation of screening [Back to SCRM Control]

The organization requires the developer of the information system, system component, or information system service take [*Assignment: organization-defined actions*] to ensure that the required access authorizations and screening criteria are satisfied.

Supplemental Guidance: Satisfying required access authorizations and personnel screening criteria includes, for example, providing a listing of all the individuals authorized to perform development activities on the selected information system, system component, or information system service so that organizations can validate that the developer has satisfied the necessary authorization and screening requirements.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-22 UNSUPPORTED SYSTEM COMPONENTS [Back to SCRM Control]

Control: The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Supplemental Guidance: Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Related controls: PL-2, SA-3.

Control Enhancements:

SA-22 (1) unsupported system components | alternative sources for continued support [Back to SCRM Control]

The organization provides [*Selection (one or more): in-house support;* [*Assignment: organization-defined support from external providers*]] for unsupported information system components.

Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES *[Back to SCRM Control]*

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

   1. System and communications protection policy [*Assignment: organization-defined frequency*]; and

   2. System and communications protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SC-1	**MOD** SC-1	**HIGH** SC-1

SC-4 INFORMATION IN SHARED RESOURCES *[Back to SCRM Control]*

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control Enhancements:

SC-5 (2) denial of service protection | excess capacity / bandwidth / redundancy [Back to SCRM Control]

The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

Supplemental Guidance: Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-5	**MOD** SC-5	**HIGH** SC-5

SC-7 BOUNDARY PROTECTION [Back to SCRM Control]

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements.

Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Control Enhancements:

SC-7 (13) boundary protection | isolation of security tools / mechanisms / support components [*Back to SCRM Control]*

The organization isolates [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Supplemental Guidance: Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations. Related controls: SA-8, SC-2, SC-3.

SC-7 (19) boundary protection | blocks communication from non-organizationally configured hosts [*Back to SCRM Control]*

The information system blocks both inbound and outbound communications traffic between [*Assignment: organization-defined communication clients*] that are independently configured by end users and external service providers.

Supplemental Guidance: Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Priority and Baseline Allocation:

P1	**LOW** SC-7	**MOD** SC-7 (3) (4) (5) (7)	**HIGH** SC-7 (3) (4) (5) (7) (8) (18) (21)

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY [*Back to SCRM Control]*

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-8 (1)	**HIGH** SC-8 (1)

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES [Back to SCRM Control]

Control Enhancements:

(1) *TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*

The information system validates the integrity of transmitted security attributes.

Supplemental Guidance: This control enhancement ensures that the verification of the integrity of transmitted information includes security attributes. Related controls: AU-10, SC-8.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-18 MOBILE CODE [Back to SCRM Control]

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements:

SC-18(1) mobile code | identify unacceptable code / take corrective actions [Back to SCRM Control]

The information system identifies [*Assignment: organization-defined unacceptable mobile code*] and takes [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.

SC-18 (2) mobile code | acquisition / development / use *[Back to SCRM Control]*

The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [*Assignment: organization-defined mobile code requirements*].

References: NIST Special Publication 800-28; DoD Instruction 8552.01.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-27 PLATFORM-INDEPENDENT APPLICATIONS *[Back to SCRM Control]*

Control: The information system includes: [*Assignment: organization-defined platform-independent applications*].

Supplemental Guidance: Platforms are combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both. Platform-independent applications are applications that run on multiple platforms. Such applications promote portability and reconstitution on different platforms, increasing the availability of critical functions within organizations while information systems with specific operating systems are under attack. Related control: SC-29.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-28 PROTECTION OF INFORMATION AT REST *[Back to SCRM Control]*

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of [*Assignment: organization-defined information at rest*].

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

References: NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-28	**HIGH** SC-28

SC-29 HETEROGENEITY *[Back to SCRM Control]*

Control: The organization employs a diverse set of information technologies for [*Assignment: organization-defined information system components*] in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations. Related controls: SA-12, SA-14, SC-27.

Control Enhancements:

SC-29(1) heterogeneity | virtualization techniques *[Back to SCRM Control]*

The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes can result in an increased work factor for adversaries in order to carry out successful cyber attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-30 CONCEALMENT AND MISDIRECTION *[Back to SCRM Control]*

Control: The organization employs [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined information systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries.

Supplemental Guidance: Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis. Related controls: SC-26, SC-29, SI-14.

Control Enhancements:

SC-30 (2) concealment and misdirection | randomness
[Back to SCRM Control]

The organization employs [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.

Supplemental Guidance: Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending against cyber attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions/business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies (e.g., browsers, search engines), using different suppliers, and rotating roles and responsibilities of organizational personnel.

SC-30 (3) concealment and misdirection | change processing / storage locations [Back to SCRM Control]

The organization changes the location of [*Assignment: organization-defined processing and/or storage*] [*Selection:* [*Assignment: organization-defined time frequency*]; *at random time intervals*]].

Supplemental Guidance: Adversaries target critical organizational missions/business functions and the information resources supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational information systems targeted by adversaries, make such systems more susceptible to cyber attacks with less adversary cost and effort to be successful. Changing organizational processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the information resources (i.e., processing and/or storage) supporting critical missions and business functions. Changing locations of processing activities and/or storage sites introduces uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational information systems much more difficult and time-consuming, and increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources.

SC-30 (4) concealment and misdirection | misleading information [Back to SCRM Control]

The organization employs realistic, but misleading information in [*Assignment: organization-defined information system components*] with regard to its security state or posture.

Supplemental Guidance: This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. As a result, adversaries may employ incorrect (and as a result ineffective) attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific security controls deployed in external information systems that are known to be accessed or targeted by adversaries. Another technique is the use of deception nets (e.g., honeynets, virtualized environments) that mimic actual aspects of organizational information systems but use, for example, out-of-date software configurations.

SC-30 (5) concealment and misdirection | concealment of system components   *[Back to SCRM Control]*

The organization employs [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined information system components*].

Supplemental Guidance: By hiding, disguising, or otherwise concealing critical information system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide and/or conceal information system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-32   INFORMATION SYSTEM PARTITIONING   *[Back to SCRM Control]*

Control: The organization partitions the information system into [*Assignment: organization-defined information system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SA-8, SC-2, SC-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-36   DISTRIBUTED PROCESSING AND STORAGE   *[Back to SCRM Control]*

Control: The organization distributes [*Assignment: organization-defined processing and storage*] across multiple physical locations.

Supplemental Guidance: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage. Related controls: CP-6, CP-7.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-37 OUT-OF-BAND CHANNELS

Control Enhancements:

SC-37 (1) out-of-band channels | ensure delivery / transmission

[Back to SCRM Control]

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that only [*Assignment: organization-defined individuals or information systems*] receive the [*Assignment: organization-defined information, information system components, or devices*].

Supplemental Guidance: Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-38 OPERATIONS SECURITY [Back to SCRM Control]

Control: The organization employs [*Assignment: organization-defined operations security safeguards*] to protect key organizational information throughout the system development life cycle.

Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details. Related controls: RA-2, RA-5, SA-12.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND INFORMATION INTEGRITY

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

[Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:

1. System and information integrity policy [*Assignment: organization-defined frequency*]; and

2. System and information integrity procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION [Back to SCRM Control]

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

SI-2(5) flaw remediation | automatic software / firmware updates [Back to SCRM Control]

The organization installs [*Assignment: organization-defined security-relevant software and firmware updates*] automatically to [*Assignment: organization-defined information system components*].

Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Organizations must balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose.

References: NIST Special Publications 800-40, 800-128.

Priority and Baseline Allocation:

P1	**LOW** SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION [Back to SCRM Control]

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

   1. Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Control Enhancements:

SI-3 (8) malicious code protection | detect unauthorized commands

[Back to SCRM Control]

The information system detects [*Assignment: organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*Assignment: organization-defined information system hardware components*] and [*Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command*].

Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from information system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by specific component, component type, location in the network, or combination therein. Organizations may select different actions for different types/classes/specific instances of potentially malicious commands. Related control: AU-6.

References: NIST Special Publication 800-83.

Priority and Baseline Allocation:

P1	**LOW** SI-3	**MOD** SI-3 (1) (2)	**HIGH** SI-3 (1) (2)

SI-4 INFORMATION SYSTEM MONITORING *[Back to SCRM Control]*

Control: The organization:

a. Monitors the information system to detect:

1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed; [Assignment: organization-defined frequency*]].

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the

Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Control Enhancements:

SI-4 (16) information system monitoring | *correlate monitoring information* [Back to SCRM Control]

The organization correlates information from monitoring tools employed throughout the information system.

Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.

SI-4 (17) information system monitoring | *integrated situational awareness* [Back to SCRM Control]

The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Supplemental Guidance: This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated cyber attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4 (16) which correlates the various cyber monitoring information, this control enhancement correlates monitoring beyond just the cyber domain. Such monitoring may help reveal attacks on organizations that are operating across multiple attack vectors. Related control: SA-12.

SI-4 (19) information system monitoring | individuals posing greater risk *[Back to SCRM Control]*

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

Supplemental Guidance: Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with federal legislation, Executive Orders, policies, directives, regulations, and standards.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

Priority and Baseline Allocation:

P1	**LOW** SI-4	**MOD** SI-4 (2) (4) (5)	**HIGH** SI-4 (2) (4) (5)

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES *[Back to SCRM Control]*

Control: The organization:

a. Receives information system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to: [*Selection (one or more): [Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	**LOW** SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTION VERIFICATION *[Back to SCRM Control]*

Control: The information system:

a. Verifies the correct operation of [*Assignment: organization-defined security functions*];

b. Performs this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]];

c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and

d. [*Selection (one or more): shuts the information system down; restarts the information system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

Supplemental Guidance: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

Control Enhancements:

SI-6 (3) security function verification | report verification results *[Back to SCRM Control]*

The organization reports the results of security function verification to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Organizational personnel with potential interest in security function verification results include, for example, senior information security officers, information system security managers, and information systems security officers. Related controls: SA-12, SI-4, SI-5.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY *[Back to SCRM Control]*

Control: The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

Control Enhancements:

SI-7 (11) software, firmware, and information integrity | confined environments with limited privileges [Back to SCRM Control]

The organization requires that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.

Supplemental Guidance: Organizations identify software that may be of greater concern with regard to origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

SI-7 (12) software, firmware, and information integrity | integrity verification [Back to SCRM Control]

The organization requires that the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.

Supplemental Guidance: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

SI-7 (13) software, firmware, and information integrity | code execution in protected environments [Back to SCRM Control]

The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software.

SI-7 (14) software, firmware, and information integrity | binary or machine executable code [Back to SCRM Control]

The organization:

(a) **Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and**

(b) **Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.**

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.

SI-7 (15) boundary protection | route privileged network accesses [Back to SCRM Control]

The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Supplemental Guidance: Related controls: AC-2, AC-3, AU-2, SI-4.

References: None.
References: NIST Special Publications 800-147, 800-155.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-7 (1) (7)	**HIGH** SI-7 (1) (2) (5) (7) (14)

SI-12 INFORMATION HANDLING AND RETENTION [Back to SCRM Control]

Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SI-12	**MOD** SI-12	**HIGH** SI-12

FAMILY: PLANNING

PL-1 SECURITY PLANNING POLICY AND PROCEDURES [Back to SCRM Control]

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:

1. Security planning policy [*Assignment: organization-defined frequency*]; and

2. Security planning procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-18, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN [Back to SCRM Control]

Control: The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization’s enterprise architecture;

2. Explicitly defines the authorization boundary for the system;

3. Describes the operational context of the information system in terms of missions and business processes;

4. Provides the security categorization of the information system including supporting rationale;

5. Describes the operational environment for the information system and relationships with or connections to other information systems;

6. Provides an overview of the security requirements for the system;

    7. Identifies any relevant overlays, if applicable;

    8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

    9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

c. Reviews the security plan for the information system [*Assignment: organization-defined frequency*];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop *overlays* for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Control Enhancements:

PL-2 (3) system security plan | plan / coordinate with other organizational entities
[Back to SCRM Control]

The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.

References: NIST Special Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-2	**MOD** PL-2 (3)	**HIGH** PL-2 (3)

PL-8 INFORMATION SECURITY ARCHITECTURE *[Back to SCRM Control]*

Control: The organization:

a. Develops an information security architecture for the information system that:

1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.

In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization’s enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.

Control Enhancements:

PL-8 (2) information security architecture | *supplier diversity*

[Back to SCRM Control]

The organization requires that [*Assignment: organization-defined security safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.

Supplemental Guidance: Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms according to their priorities and development schedules. By having different products at different locations (e.g., server, boundary, desktop) there is an increased likelihood that at least one will detect the malicious code. Related control: SA-12.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PL-8	**HIGH** PL-8

FAMILY: PROGRAM MANAGEMENT

PM-1 INFORMATION SECURITY PROGRAM PLAN *[Back to SCRM Control]*

Control: The organization:

a. Develops and disseminates an organization-wide information security program plan that:

   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

   3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and

   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*];

c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

d. Protects the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any *assignment* and *selection* statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization’s information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Control Enhancements: None.

References: None.

PM-2 SENIOR INFORMATION SECURITY OFFICER [Back to SCRM Control]

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

References: None.

PM-3 INFORMATION SECURITY RESOURCES [Back to SCRM Control]

Control: The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

PM-11 MISSION/BUSINESS PROCESS DEFINITION [Back to SCRM Control]

Control: The organization:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60.

PM-16 THREAT AWARENESS PROGRAM [Back to SCRM Control]

Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.

Control Enhancements: None.

References: None

APPENDIX E

ICT SUPPLY CHAIN THREAT EVENTS

Appendix E provides examples of ICT supply chain threat events. These examples are based on NIST SP 800-30 Rev1 Appendix E, *Threat Events*. Specifically, Tables E-2, *Representative Examples – Adversarial Threat Events*, and E-3, *Representative Examples – Non-Adversarial Threat Events*, were used to create the two corresponding tables in this document. It should be noted that the threat events in NIST SP 800-30 Rev1 Appendix E are generic threat events that were tailored to information security rather than ICT SCRM context. The tables used as source material for this appendix contain 2 columns – Threat Events and Description.

The generic threats in NIST SP 800-30 Rev1, Appendix E, are at times quite broad and needed to be further specified to be ICT supply chain-specific for use in this document. This document lists only those threats events that are relevant to ICT supply chain in all or under some circumstances. To indicate when the threat events are relevant only under some but not all circumstances, a comment is included the third column, Comments, to provide the rationale for when the specific threat event is relevant to ICT supply chain.

Organizations may use the examples of ICT supply chain threat events provided in this appendix during threat analysis described in Chapter 2, if appropriate.

Table E-1. Adversarial ICT Supply Chain Threat Events

Threat Events (Characterized by TTPs)	Description	Comments
Perform reconnaissance and gather information.		
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.	
Craft or create attack tools.		
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means, commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.	

Threat Events (Characterized by TTPs)	Description	Comments
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.	
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.	
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.	
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain.	
Deliver/insert/install malicious capabilities.		
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.	
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.	
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.	
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.	
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.	

Threat Events (Characterized by TTPs)	Description	Comments
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).	
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.	
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.	
Insert tampered critical components into organizational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.	
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.	
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.	YES, if the individual is placed by an external party.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.	
Exploit and compromise.		

Threat Events (Characterized by TTPs)	Description	Comments
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections.	YES, if information systems are those belonging to external organization.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.	YES, if the threat is to ICT supply chain.
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).	
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.	
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.	
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.	
Conduct an attack (i.e., direct/coordinate attack tools or activities).		
Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).	

Threat Events (Characterized by TTPs)	Description	Comments
Conduct internally based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.	YES, for critical systems.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.	
Achieve results (i.e., cause adverse impacts, obtain information)		
Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.	YES, because this may be related to information-sharing agreements.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.	YES, because this originates externally.
Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.	YES, if an adversary is not an employee.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e.g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.	
Maintain a presence or set of capabilities.		
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.	YES, if these are multiple organizations composing ICT supply chain.

Threat Events (Characterized by TTPs)	Description	Comments
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.	

Table E-1. Adversarial ICT Supply Chain Threat Events

Threat Event	Description	Comments
Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.	
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.	YES, if user is not an employee.
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.	YES, if user is not an employee.
Resource depletion	Degraded processing performance due to resource depletion.	YES, if physical resources are being depleted. YES, if resources of an external service provider are being depleted.

Threat Event	Description	Comments
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.	
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.	

APPENDIX F

SUPPLY CHAIN THREAT SCENARIOS AND ANALYSIS FRAMEWORK

ICT supply chain risk management is an enterprise process with a significant number of moving parts that simultaneously and sequentially impact various systems and elements through both manual and automated processes. Because the supply chain covers the entire life cycle of a system/element, there are numerous opportunities for vulnerabilities that impact the environment or the system/element to be intentionally or unintentionally inserted, created, or exploited. **A Threat Scenario is a summary of potential consequence(s) of the successful exploitation of a specific vulnerability or vulnerabilities by a threat agent.** They help organizations analyze the likelihood and impact a specific event would have on an organization and identify appropriate mitigating strategies.

Threat scenarios are generally used in two ways:

1. To translate the often disconnected information garnered from a risk assessment, such as described in NIST SP 800-30, into a more tangible, story-like situation for further evaluation. These stories can help organizations discover additional vulnerabilities requiring mitigation and used for training; and

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

These scenarios can then be used to identify areas requiring increased controls and for training purposes. By performing an in-depth analysis of how a specific event will impact an organization using a threat scenario, relationships and dependencies that might otherwise be overlooked during the risk assessment can become visible and appropriate mitigating strategies employed.

Because threat scenarios focus on specific, often hypothetical, events, they should not be used to replace a more traditional, holistic risk assessment. Rather, they should be used as a tool to further evaluate specific vulnerabilities or areas of concern. Due to the infinite number of possible scenarios and directions into which a threat scenario can evolve, it is important to have a structured approach with well-defined goals and scope.

This section provides an example of a generic threat scenario analysis framework for ICT SCRM that can be used by organizations to develop a framework that best suits their needs. It also contains four examples of how this framework may be used. The examples differ slightly in their implementation of the framework so as to show how the framework may be tailored. Each example identifies one or more vulnerabilities, describes a specific threat source, identifies the expected impact on the organization, and proposes SP 800-161 SCRM controls that would help mitigate resulting risk.

Developing and Analyzing Threat Scenarios & Identifying Applicable Controls

Step 1: Create a Plan for Developing and Analyzing Scenarios

- Identify the purpose of the Threat Scenario Analysis in terms of the objectives, milestones, and expected deliverables;
- Identify the scope of organizational applicability, level of detail, and other constraints;
- Identify resources to be used, including personnel, time, and equipment; and
- Define a framework to be used for analyzing scenarios.

Step 2: Characterize the Environment

- Identify core business/mission processes and key organizational dependencies;
- Describe threat sources that are relevant to the organization. Include the motivation and resources available to the threat source, if applicable;
- List known vulnerabilities or areas of concern (Note: Examples of areas of concern include the planned outsourcing of a manufacturing plant, the pending termination of a maintenance contract, or the discontinued manufacture of an element.);
- Identify existing and planned controls; and
- Identify related regulations, standards, policies, and procedures.

Step 3: Develop and Select Threat Event(s) for Analysis

- List possible ways threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events (Note: Historical data is useful in determine this information.);
- Briefly outline the series of consequences that could occur as a result of each threat event. These may be as broad or specific as necessary. If applicable, estimate the likelihood and impact of each event;
- Eliminate those events that are clearly outside the defined purpose and scope of the analysis;
- Describe in more detail the remaining threat events. Include the tactics, techniques, and procedures used to carry out attacks (Note: The level of detail in the description is dependent on the needs of the organization.); and
- Select for analysis those events that best fit the defined purpose and scope of the analysis. More likely events, events of special concern, and an event that can represent several of the other listed events are generally useful candidates.

Step 4: Conduct the Threat Scenario Analysis

- For each threat event, note any immediate consequences of the event and identify those organizational units and processes that would be affected, taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures;
- Estimate the impact these consequences would have on the mission / business processes as well as the organizational units affected, preferably in quantitative terms from historical data and taking into account existing and planned controls, and applicable regulations, standards, policies and procedures (Note: It may be beneficial to identify a “most likely” impact level and a “worst-case” or “100-year” impact level.); and

- Identify those organizational units or processes that would be subsequently affected, the consequences and the impact levels, until each affected process has been analyzed, taking into account existing and planned controls, and applicable regulations, standards, policies and procedures (e.g., If a critical server goes down, one of the first processes affected may be the technology support department, but if they determine a new part is needed to bring the server back up, the procurement department may become involved.).

Step 5: Determine Applicable Controls

- Determine the level of risk (impact and likelihood) that is acceptable to the organization for each analyzed Threat Event (Note: In some cases, the level of acceptable risk may be dependent on the cost of mitigating strategies.);
- Compare the level of acceptable risk to the existing level of risk as determined by the threat scenario analysis;
- Identify potential mitigating controls (Note: Using a list of standard or recommended controls such as those found in NIST SP 800-53 can make this process simpler.);
- Estimate the effectiveness of those controls at reducing the risk of a scenario;
- Estimate the resources needed (in terms of money, personnel, time) to implement potential controls; and
- Identify those controls or combinations of controls that would cause the estimated residual risk of a threat event to drop to an acceptable level in the most resource-effective manner, taking into account any rules or regulations that may apply (Note: Consideration should be given to the potential that one control will help mitigate the risk from more than one event, or that a control may increase the risk of a separate event.).

Step 6: Evaluate / Feedback

- Develop a plan to implement the selected controls and evaluate their effectiveness; and
- Evaluate the effectiveness of the threat scenario analysis and make improvements as needed.

Sample Threat Scenario Analysis Framework

Threat Scenario	Threat Source	
	Vulnerability	
	Threat Event Description	
	Outcome	
Organizational units / processes affected		
Risk	Impact	
	Likelihood	
	Risk Score (Impact x Likelihood)	
	Acceptable Level of Risk	
Mitigation	Potential Mitigating Strategies / SCRM Controls	
	Estimated Cost of Mitigating Strategies	
	Change in Likelihood	
	Change in Impact	
	Selected Strategies	
	Estimated Residual Risk	

Sample Scenarios

This section provides four example threat scenarios specific to the U.S. government using the generic framework described above. The examples purposely vary in level of specificity and detail to show that threat scenarios can be as broad or specific, as detailed or generic, as necessary. While these scenarios use basic scoring measures (High, Moderate, Low) for likelihood, impact, and risk, organizations may use any of a number of different units of measure (e.g., percentage, CVSS score, etc.). Additionally, these scenarios vary slightly in implementation of the framework to show that the framework can be adapted as needed.

Scenario 1: Telco Counterfeits

Background:

A large U.S. government agency has developed a system which is maintained through contract by an external integration company. The system requires a common telecommunications element that is no longer available from the Original Component Manufacturer (OCM). The OCM has offered a newer product as a replacement, but it would require modifications to the system at a cost of approximately $1 million. If the element is not upgraded, the agency and system integrator would have to rely on secondary market suppliers for replacements. The newer product provides no significant improvement on the element currently being used.

The USG agency has decided to perform a threat scenario analysis to determine whether to modify the system to accept the new product, or accept the risk of continuing to use a product that is no longer in production.

Environment

The environment is characterized as follows:

- The system is expected to last ten more years without any major upgrades / modifications and has a 99.9% uptime requirement.
- Over 1,000 of the $200 element are used throughout the system and approximately 10% are replaced every year due to regular wear-and-tear, malfunctions, or other reasons. The integrator has approximately a three-month supply on hand at any time.
- The element is continuously monitored for functionality, and efficient procedures exist to reroute traffic and replace the element should it unexpectedly fail.
- Outages resulting from unexpected failure of the element are rare, localized, and last only a few minutes. More frequently, when an element fails, the system’s functionality is severely reduced for approximately one-to four-hours while the problem is diagnosed and fixed or the element replaced.
- Products such as the element in question have been a common target for counterfeiting.
- The integrator has policies restricting the purchase of counterfeit goods and a procedure to follow if a counterfeit is discovered (SCRM_SA-16).
- The integrator and acquiring agency have limited testing procedures to ensure functionality of the element before acceptance [SA-10 (4)].

Threat Event

To support the threat scenario, the agency created a fictitious threat source described as a group motivated by profit with vast experience creating counterfeit solutions. The counterfeiter is able to make a high profit margin by creating and selling as genuine, products that are visually identical to their genuine counterparts but which use lower-quality materials. They have the resources to copy most trademark and other identifying characteristics and insert counterfeits into a supply chain commonly used by the USG with little to no risk of detection. The counterfeit product is appealing to unaware purchasing authorities as it is generally offered at a discount - sold as excess inventory or as stockpile.

If an inferior quality element was inserted into the system, it would likely fail more often than expected, causing reduced functionality of the system. In the event a large number of counterfeit products were mixed in with genuine parts and integrated into the system randomly, the number and severity of unexpected outages could grow significantly. The agency and integrator decided that the chances a counterfeit product could be purchased to maintain the system and the estimated potential impact of such an event were high enough to warrant further evaluation.

Threat Scenario Analysis

The person(s) purchasing the element from a supplier will be the first affected by a counterfeit product. Policy dictates that they attempt to purchase a genuine product from trusted suppliers. This person will have to be led to believe that the product is genuine. As the counterfeit product in question is visually identical to the element desired, and at a discount, there is a high chance the counterfeit will be purchased. One will be tested to ensure functionality, and then the items will be placed into storage.

When one of the elements in the system needs to be replaced, an engineer will install a counterfeit, quickly test to ensure it is running properly, and record the change. It could take two years for the counterfeit product to fail, so up to 200 counterfeit elements could be inserted into the system before the first one fails. If all the regularly replaced elements are substituted for counterfeits and each counterfeit fails after two years, the cost of the system would increase by $160,000 in ten years. The maintenance time required would also cost the integration company in personnel and other expenses.

When a counterfeit fails, it will take approximately one-to four hours to diagnose and replace the element. During this time, productivity is severely reduced. If more than one of the elements fails at the same time, the system could fail. This could cause significant damage to agency operations and violate the 99.9% uptime requirements set forth in the contract. Plus, if it is determined that the element failed because it was a counterfeit, there would be additional costs associated with reporting the counterfeit.

Mitigation Strategy:

The following were identified as potential mitigating activities (from NIST SP 800-161):

- Require developers perform security testing/evaluation at all post-design phases of the SDLC [SCRM_SA-9];
- Validate that the information system or system component received is genuine and has not been altered [SCRM_SA-10 (7)];

- Incorporate security requirements into the design of information systems (defensive design) [SCRM_PL-3, SCRM_SC-13]; and
- Employ supplier diversity requirements [SCRM_PL-3(1)].

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

- Acceptance testing: Examination of elements to ensure that they are new, genuine, and that all associated licenses are valid;
- Increase security requirements into the design of the system by adding redundant elements along more critical paths in order to minimize the impact of an element failure; and
- Search for alternative suppliers / components.

It was determined that this strategy would cost less than accepting the risk of allowing counterfeits into the system or modifying the system to accept the upgraded element. The estimated cost for implementing a more rigorous acquisition and testing program was $80,000; the cost for increasing defensive design requirements was $100,000.

Threat Scenario	**Threat Source:**	Counterfeit telecommunications element introduced into supply chain.		
	Vulnerability:	Element no longer produced by OCM. Purchasing authorities unable / unwilling to identify and purchase only genuine elements.		
	Threat Event Description:	Threat agent inserts their counterfeit element into a trusted distribution chain. → Purchasing authorities buy the counterfeit element. → Counterfeit elements installed into the system.		
	Outcome:	The element fails more frequently than before, increasing the number of outages.		
Organizational units / processes affected:		Acquisitions Maintenance OCM / supplier relations Mission-essential functions		
Risk	**Impact:**	High - Outages increase by 80%	Medium – Outages increase by 40%	Low – outages increase by 10%
	Likelihood:	15%	40%	45%
	Risk Score (Impact x Likelihood):	High		
	Acceptable Level of Risk:	Low		
Mitigation	**Potential Mitigating Strategies / SCRM Controls:**	Increase acceptance testing capabilities [SCRM_SA-9; SCRM_SA-10 (7)], increase security requirements in design of systems [SCRM_PL-3, SCRM_SC-13], and employ supplier diversity requirements [SCRM_PL-3(1)].	Modify the system to accept element upgrade.	
	Estimated Cost of Mitigating Strategies:	$180,000	$1million	
	Change in Likelihood:	Low	Large	
	Change in Impact:	Moderate	None	
	Selected Strategies:	Agency-level examination and testing. Place elements in escrow until they pass acceptance testing. Increase the defensive design. Search for multiple suppliers of the element.		
	Estimated Residual Risk:	Low		

Scenario 2: Industrial espionage.

Background:

Harlow Inc., a semiconductor (SC) company used by the USG to produce military and aerospace systems, is considering a partnership with a KXY Co. to leverage their fabrication facility. This would represent a significant change in the supply chain related to a critical system element. A committee was formed including representatives from the USG organization, Harlow Inc., and the integration company to help identify the impact the partnership would have on the USG and risk-appropriate mitigating practices to enact when the partnership is completed.

Environment:

The systems of concern are vital to the safety of military and aerospace missions. While not classified, the element KXY would be expected to manufacture is unique, patented, and critical to the operational status of the systems. Loss of availability of the element while the system is operational could have significant, immediate impact across multiple agencies and the civilian populous, including loss of life and millions of dollars in damages. The existing level of risk for this is was given a score of “Moderate.”

KXY currently produces a state-of-the-art, low-cost wafer fabrication whose focus is primarily commercial. The nation-state in which KXY operates has a history of conducting industrial espionage to gain IP / technology. They have shown interest in semiconductor technology and provided a significant grant to KXY to expand into the military and aerospace markets. While KXY does not currently have the testing infrastructure to meet U.S. industry compliance requirements, the nation-state’s resources are significant, including the ability to provide both concessions as well as incentives to help KXY meet those requirements.

The key area of concern was that the nation-state in which KXY operates would be able to use its influence to gain access to the element or the element’s design.

The committee reviewed current mitigation strategies in place and determined that Harlow, Inc., the integration company, and the USG organization had several existing practices to ensure that the system and all critical elements met specific functionality requirements. For example, the system and critical elements underwent rigorous testing for compliance with industry standards. As part of their requirements under NIST SP 800-53 rev. 4, the agency had some information protection requirements (SCRM_PM-4). In addition, Harlow, Inc., had a sophisticated inventory tracking system that required that most elements be uniquely tagged or otherwise identified for traceability (SCRM_SA-10 (11)).

Threat Scenario:

Based on past experience, the USG organization decided that KXY’s host nation would likely perform one of two actions if given access to the technology: sell it to interested parties or insert / identify vulnerabilities for later exploitation. For either of these threat events to be successful, the host nation would have to understand the purpose of the element and be given significant access to the element or element's design. This could be done with cooperation of KXY's human resources department, through deception, or by physical or electronic theft. Physical theft would be difficult given existing physical control requirements and inventory control procedures. For a modified element to be purchased and integrated with the system, it would need to pass testing procedures at both the integrator and agency level. Modifications to identification labels / schemes would need to be undetectable in a basic examination. In addition, KXY would need to pass routine audits which would check KXY's processes for ensuring the quality and functionality of the element.

- The committee decided that, despite existing practices, there was a 30% chance that the host nation would have the motivation and ability to either develop harmful modifications to the element without detection, exploit previously unknown vulnerabilities, or provide the means for one of their allies to do the same. This could result in a loss of availability or integrity of the system, causing significant harm. The USG has identified this as the worst-case scenario with an impact score of "High."

- There is approximately a 40% chance that the host nation could and would sell the technology to interested parties, resulting in a loss of technological superiority. If this scenario occurred, friendly military and civilian lives could be at risk, intelligence operations would be damaged, and more money would be required to invest in a new solution. The impact score for this scenario was given a score of "Moderate."

The overall combined risk score for the vulnerability of concern was determined to be "High."

Mitigating strategies:

Using SP 800-161 controls, four potential strategies were identified by the committee: (1) modify identification methods to better prevent alterations or theft, (2) increase access practice requirements, (3) increase requirements for maintaining provenance, and (4) choose another supplier. These four options were analyzed in more detail to determine their impact on the scenarios and their estimated cost to implement.

Using NIST SP 800-161 as a base, three broad strategies were identified by the committee: (1) improve traceability capabilities, (2) increase provenance and information requirements, and (3) choose another supplier. These three options were analyzed in more detail to determine their impact on the scenarios and their estimated cost to implement.

1) Improve traceability and monitoring capabilities.
    a. SCRM_CM-8 - INFORMATION SYSTEM COMPONENT INVENTORY
    b. SCRM_IA-1 - IDENTIFICATION AND AUTHENCITCATION POLICY AND PROCEDURES
    c. SCRM_SA-8 (1) - DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION
    d. SCRM_SA-8 (3) - DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION

    e. SCRM_SA-10 (7) - SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED
    f. SCRM_SA-10 (11) - SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY
    g. Cost = 20% increase
    h. Impact = 10% decrease

2) Increase provenance and information control requirements.
    a. SCRM_AC-11 - COLLABORATION AND INFORMATION SHARING
    b. SCRM_PV-1 - PROVENANCE POLICY AND PROCEDURES
    c. SCRM_PV-2 - BASELINING AND TRACKING PROVENANCE
    d. Cost = 20% increase
    e. Impact = 20% decrease
3) Choose another supplier.
    a. SCRM_SA-10 (2) - SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS
    b. Cost = 40% increase
    c. Impact = 80% decrease

Based on this analysis, the committee decided to implement a combination of practices:

- Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component. [SCRM_SA-10 (3)]
- Minimize the amount of information that is shared to suppliers. Require that the information be secured. [SCRM AC-11]
- Require provenance be kept and updated throughout the SDLC. [SCRM_PV-1]

With this combination of controls, the estimated residual risk was determined to be equivalent with the existing risk without the partnership at a cost increase that is less than if the organization changed suppliers.

Threat Scenario	**Threat Source:**	Nation-state with significant resources looking to steal IP		
	Vulnerability :	Supplier considering partnership with company that has relationship with threat source.		
	Threat Event Description:	• Nation-state helps KXY meet industry compliance requirements. • Harlow, Inc. partners with KXY to develop chips.		
	Existing Practices:	• Strong contractual requirements as to the functionality of the system and elements • Comprehensive inventory tracking system at Harlow, Inc. • Industry compliance requirements		
	Outcome:	• Nation-state extracts technology threat actor modifies technology or exploits previously unknown vulnerability		
Organizational units / processes affected:		• KXY Supplier • Harlow, Inc. / integrator functionality testing • Technology users • Other USG agencies / customers		
Risk	**Impact:**	Technology modified / vulnerabilities exploited – High	Technology sold to interested parties - Moderate	
	Likelihood:	Moderate	Moderate	
	Risk Score (Impact x Likelihood):	High		
	Acceptable Level of Risk:	Moderate		
Mitigation	**Potential Mitigating Strategies / SCRM Controls:**	(1) Improve traceability and monitoring capabilities	(2) Increase provenance and information control requirements	(3) choose another supplier
	Estimated Cost of Mitigating Strategies:	20% increase	20% increase	40% increase
	New Risk Score:	Moderate	Moderate	Moderate
	Selected Strategies:	• Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component. [SCRM_SA-10 (3)] • Minimize the amount of information that is shared to suppliers. Require that the information be secured. [SCRM AC-11] • Require provenance be kept and updated throughout the SDLC. [SCRM_PV-1]		
	Estimated Residual Risk:	Moderate - The residual risk was determined to be equivalent with the existing risk without the partnership.		

Scenario 3: Malicious Code Insertion

Background:

A USG organization has decided to perform a threat scenario analysis on a traffic control system. The scenario is to focus on software vulnerabilities and should provide general recommendations regarding mitigating practices.

Environment:

The system runs nearly automatically and uses computers running a commonly available operating system along with centralized servers. The software was created in-house and is regularly maintained and updated by an integration company on contract for the next five years. The integration company is large, frequently used by the USG in a variety of projects, and has significant resources to ensure that the system maintains its high availability and integrity requirements.

Threats to the system could include: loss of power to the system, loss of functionality, or loss of integrity causing incorrect commands to be processed. Some threat sources could include nature, malicious outsiders, and malicious insiders. The system is equipped with certain safety controls such as back-up generator power, redundancy of design, and contingency plans if the system fails.

Threat Event:

The organization decided that the most concerning threat event would be if a malicious insider were to compromise the integrity of the system. Possible attacks were that the threat actor could insert a worm or a virus into the system, reducing its ability to function, or they could manually control the system from one of the central servers or by creating a back-door in the server to be accessed remotely. Depending on the skillfulness of the attack, an insider could gain control of the system, override certain fail-safes, and cause significant damage.

Based on this information, the organization developed the following fictitious threat event to be analyzed:

> John Poindexter, a disgruntled employee of the integration company, decides to insert some open-source malware into a component of the system. He then resigns from the firm, leaving no traceability of his work. The malware has the ability to call home to John and provides him access to stop or allow network traffic at any or all 50 of the transportation stations. As a result, there would be unpredictable, difficult-to-diagnose disruptions, causing significant monetary losses and safety concerns.

Management has decided that the acceptable level of risk for this scenario is “Moderate.”

Threat Scenario Analysis:

If John were successful, a potential course of events would be as follows:

> John conducts a trial run – shutting off the services of one station for a short time. It would be discounted as a fluke and have minimal impact. Later, John would create increasingly frequent disruptions at various stations. These disruptions would cause anger among employees and customers and some safety concerns. The integration company would be made aware of problem and begin to investigate the cause. They would create a work-around, assuming there was a bug in the system. However, because the malicious code would be buried and difficult to identify, the integration company wouldn’t discover it. John would then create a major disruption across several transportation systems at once. The work-around created by the integration company would fail due to the size of the attack, and all transportation services would be halted. Travelers would be severely impacted, and the media alerted. The method of attack would be identified and the system modified to prevent John from accessing the system again. However, the underlying malicious code would remain. Revenue would decrease significantly for several months. Legal questions would be raised. Resources would be invested in ensuring the public that the system was safe.

Mitigating Practices:

The organization identified the following as potential areas for improvement:

- Establish and retain identification of supply chain elements, processes, and actors – SCRM_SA-10 (11);
- Control access and configuration changes within the SDLC - SCRM_AC-1, SCRM_ AC-2, SCRM_CM-3;
- Require static code testing - SCRM_SA-11 (1); and
- Incident Response Handling - SCRM_IR-2.

Threat Scenario	**Threat Source:**	Integrator– Malicious Code Insertion
	Vulnerability:	Minimal oversight of integrator activities - no checks and balances for any individual inserting a small piece of code.
	Threat Event Description:	Disgruntled employee of an Integrator company inserts malicious functionality into traffic navigation software, and then leaves the company.
	Existing Practices:	Integrator: peer-review process Acquirer: Contract that sets down time, cost, and functionality requirements
	Outcome:	50 large metro locations and 500 instances affected by malware. When activated, the malware causes major disruptions to traffic.
Organizational units / processes affected:		Traffic Navigation System Implementation company Legal Public Affairs
Risk	**Impact:**	High – Traffic disruptions are major and last for two weeks while a work-around is created. Malicious code is not discovered and remains a vulnerability.
	Likelihood:	High
	Risk Score (Impact x Likelihood):	High
	Acceptable Level of Risk:	Moderate
Mitigation	**Potential Mitigating Strategies / SCRM Controls:**	SCRM_AC-1; SCRM_ AC-2; SCRM_CM-3; SCRM_IR-2; SCRM_SA-10(11); SCRM_SA-11(1)
	Estimated Cost of Mitigating Strategies:	$2.5Mil
	Change in Impact:	Large
	Change in Likelihood:	Large
	Selected Strategies:	Combination of strategies using the mitigation noted
	Estimated Residual Risk:	Moderate

Scenario 4: Unintentional Compromise

Background:

Uninformed insiders replace components with more cost-efficient solutions without understanding the implications to performance, safety, and long-term costs.

A USG agency has concerns about its acquisition policies and has decided to conduct a threat scenario analysis to identify applicable mitigating practices. Any practices selected must be applicable to a variety of projects and have significant success within a year.

Environment:

The agency acquires many different systems with varying degrees of requirements. Because of the complexity of the environment, agency officials decided that they should use a scenario based on an actual past event.

Threat Event:

Modifying an actual event, the agency designed the following threat event narrative:

> Gill, a newly hired program manager, is tasked with reducing the cost of a $5 million system being purchased to support complex research applications in a unique physical environment. The system would be responsible for relaying information regarding temperature, humidity, and toxic chemical detection as well as for storing and analyzing various data sets. There must not be any unscheduled outages more than 10 seconds long or there will be serious safety concerns and potential destruction of research. The agency has determined that the acceptable level of risk for this type of event has a score of 2/10.
>
> Gill sees that a number of components in the system design are priced high compared with similar components he has purchased in the commercial acquisition space. Gill asks John, a junior engineer with the integration company, to replace several load balancer / routers in the system design to save costs.

Threat Scenario Analysis:

The agency decided that there were three potential outcomes to the scenario:

1. It is determined that the modifications are inadequate before any are purchased (30% chance, no impact);
2. It is determined that the modifications are inadequate during testing (40% chance, low impact); or
3. The inadequacy of the modifications is undetected, the routers are installed in the system, begin to fail, and create denial of service incidents (30% chance, high impact).

Mitigating strategies:

Three potential mitigating strategies were identified:

1. Improve the existing training program (SCRM_AT-1);
2. Improve the testing requirements (SCRM_SA-9); and
3. Require redundancy and heterogeneity in the design of systems (SCRM SC-13, SCRM_SC-10).

Improving the training program would increase the likelihood that the modifications are rejected either at the initial stage or during testing, but it was determined that a $200,000 investment in training alone could not bring the level of risk to an acceptable level in the time required.

Improving the testing requirements would increase the likelihood that the modifications are rejected during testing, but it was determined that no amount of testing alone could bring the level of risk to an acceptable level.

Requiring redundancy and heterogeneity in the design of the system would significantly reduce the impact of this and other events of concern, but could double the cost of a project. In this scenario, it was determined that an investment of $2 million would be required to bring the risk to an acceptable level.

As a result of this analysis, the agency decided to implement a combination of practices:

- A mandatory, day-long training program for those handling the acquisition of critical systems ($80,000 initial investment);
- $60,000 investment in testing equipment and software for critical systems and elements; and
- Redundancy and diversity of design requirements as deemed appropriate for each project.

It was determined that this combination provided a series of practices that would be most cost-effective for a variety of projects and would also help mitigate the risk from a variety of threats.

<table>
<tr><td rowspan="5">Threat Scenario</td><td><b>Threat Source:</b></td><td colspan="9">Internal Employee – Unintentional Compromise</td></tr>
<tr><td><b>Vulnerability:</b></td><td colspan="9">Lax training practices</td></tr>
<tr><td><b>Threat Event Description:</b></td><td colspan="9">A new acquisition officer (AO) with experience in commercial acquisition is tasked with reducing hardware costs. The AO sees that a number of components are priced high and works with an engineer to change the purchase order.</td></tr>
<tr><td><b>Existing Practices:</b></td><td colspan="9">Minimal training program that is not considered mandatory
Basic testing requirements for system components</td></tr>
<tr><td><b>Outcome:</b></td><td colspan="3">Change is found unsuitable before purchase</td><td colspan="3">Change is found unsuitable in testing</td><td colspan="3">Change passes testing, routers installed and start to fail, causing a denial of service situation.</td></tr>
<tr><td colspan="2"><b>Organizational units / processes affected:</b></td><td colspan="3">None</td><td colspan="3">Acquisitions</td><td colspan="3">Acquisitions, System, Users</td></tr>
<tr><td rowspan="4">Risk</td><td><b>Impact:</b></td><td colspan="3">None</td><td colspan="3">Low</td><td colspan="3">High</td></tr>
<tr><td><b>Likelihood:</b></td><td colspan="3">30%</td><td colspan="3">30%</td><td colspan="3">40%</td></tr>
<tr><td><b>Risk Score (Impact x Likelihood):</b></td><td colspan="9">High</td></tr>
<tr><td><b>Acceptable Level of Risk:</b></td><td colspan="9">Low</td></tr>
<tr><td rowspan="8">Mitigation</td><td><b>Potential Mitigating Strategies / SCRM Controls:</b></td><td colspan="3">Improve training program</td><td colspan="3">Improve acquisition testing</td><td colspan="3">Improve design of system</td></tr>
<tr><td><b>Estimated Cost of Mitigating Strategies:</b></td><td colspan="3">$200,000</td><td colspan="3">---</td><td colspan="3">$2 million</td></tr>
<tr><td><b>Change in Impact:</b></td><td colspan="3">None</td><td colspan="3">None</td><td colspan="3">Significant</td></tr>
<tr><td><b>Change in Likelihood:</b></td><td>+10%</td><td>+10%</td><td>-20%</td><td>0</td><td>+20%</td><td>-20%</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td><b>New Risk Score:</b></td><td colspan="3">4/10</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td><b>Selected Strategies:</b></td><td colspan="9">Make training program mandatory for those working on critical systems. (Cost = $60,000)</td></tr>
<tr><td><b>Residual Risk:</b></td><td colspan="9">Low</td></tr>
</table>