
**ITL BULLETIN FOR NOVEMBER 2012**

## PRACTICES FOR MANAGING SUPPLY CHAIN RISKS TO PROTECT FEDERAL INFORMATION SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Many organizations rely on complex information systems that are composed of hardware, software, and firmware products developed by different system developers, suppliers, and integrators. The information and communications technology (ICT) supply chain is a globally distributed, interconnected set of organizations, people, processes, products, and services. It extends across the full system development life cycle (SDLC) including research and development (R&D), design, development, acquisition of custom or commercial off-the-shelf (COTS) products, delivery, integration, operations, and disposal/retirement.

The modern ICT supply chain is subject to a variety of cyber security threats. These threats may affect the confidentiality, integrity, or availability of government information and information systems and include counterfeiting, tampering, theft, reduced or unwanted functionality, or malicious content. Without effective security processes and practices throughout the life cycle of a system, intentional and unintentional vulnerabilities can be placed into systems. The systems then may be exploited by attackers who insert malicious content, capture data, or take other advantages, resulting in untrustworthy products or services, unanticipated failure rates, or compromise of federal missions and information.

Federal information systems are increasingly at risk to both intentional and unintentional supply chain compromises because of the growing sophistication of ICT and the complexity, scale, and speed of a distributed global supply chain. Failure to address the obscure processes and practices used to create and deliver hardware and software products and services can result in vulnerability to threats throughout the system development life cycle.

### NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*

NISTIR 7622 provides federal departments and agencies with a notional set of repeatable and commercially reasonable supply chain assurance methods and practices to strategically manage ICT supply chain risks over the life cycle of ICT systems, products, and services. The document discusses ICT supply chain challenges and foundational practices, and provides information on how ICT supply chain risk management (SCRM) considerations can be integrated into the

federal acquisition life cycle. The publication was written by Jon Boyens and Celia Paulsen of NIST, Nadya Bartol and Stephanie Shankles of Booz Allen Hamilton, and Rama Moorthy of Hatha Systems.

Many of the ICT supply chain risk management activities described build on existing practices already used by government and industry organizations. They include business and engineering processes from many disciplines including logistics, reliability, security, and safety. The specific ICT SCRM practices are directed toward federal department and agency acquirers.

These practices are recommended for use in information systems that are categorized at the Federal Information Processing Standard (FIPS) 199 high-impact level. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Federal agencies may choose to apply the practices recommended to specific systems with a lower impact level, based on the tailoring guidance provided in draft NIST Special Publication (SP) 800-53 Rev.4, *Recommended Security Controls for Federal Information Systems*. See the **For Information Section** below for details on accessing this publication.

Appendices to the publication provide a glossary of terms used, the acronyms and abbreviations used, and a list of references for ICT SCRM. One section summarizes a study on supply chain management that was performed by the University of Maryland's Supply Chain Management Center on a grant from NIST.

**Recommended Supply Chain Risk Management Practices**

NISTIR 7622 recommends that federal departments and agencies consider the following practices when they develop their supply chain risk management policies. These recommended practices are consistent with current and emerging international consensus-based standards, and apply to the entire system development life cycle.

• **Uniquely identify supply chain elements, processes, and people involved**. Supply chain elements include off-the-shelf software, hardware, and firmware, including components, devices, products, systems, and materials. Processes include a variety of business or engineering processes such as logistics, reliability, security, and safety that are used by many business and government organizations. The people involved include the federal department or agency acquiring the product or service; the supplier of products, systems and system components; and the integrator organizations that combine, add, and optimize the elements, processes, and systems. Knowledge and understanding of these components will help federal departments and agencies monitor and manage risk and reduce the likelihood of an adverse event.


• **Limit access and exposure within the supply chain**. Many people may have access to the software, hardware, and firmware elements of the supply chain. To minimize risk, the access of people and organizations should be limited to those elements that are needed for the performance of valid assigned roles and duties, and access should be monitored for impact on the supply chain. Existing access control techniques may be useful in ensuring that only appropriate people or organizations can monitor or change supply chain elements, element processes, organizations, organizational processes, information, communications, and systems covering the comprehensive supply chain.

• **Establish and maintain the provenance of elements, processes, tools, and data.** The record of the origin of system elements, changes to elements, and who made the changes is called *provenance.* Acquirers, integrators, and suppliers should maintain the provenance of elements under their control. Provenance is used to ascertain the source of goods such as computer hardware to assess if they are genuine or counterfeit, and provenance allows for all changes from the baselines of components, component processes, information, systems, organizations, and organizational processes, to be appropriately reported. This provides for greater traceability in case of an adverse event and for effective risk management. Changes to objects and activities within a supply chain and the persons, organizations, or processes responsible for authorizing and performing such changes should be inventoried, monitored, recorded, and reported.

• **Share information within strict limits.** Acquirers, integrators, and suppliers need to share data and information that can span the entire system or element life cycle and the entire supply chain. Content to be shared may include data and information about the use of elements, users, acquirer, integrator, or supplier organizations, as well as information regarding issues that have been identified about specific elements. Information should be protected according to mutually agreed-upon practices that allow information to reach specified individuals and organizations in quantity, quality, and with timeliness to enable the performance of required tasks and functions.

• **Perform supply chain risk management awareness and training.** Federal department and agency acquirer personnel and integrator personnel need training on supply chain policy, procedures, and applicable management, operational, and technical controls and practices. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, provides guidelines for establishing and maintaining a comprehensive awareness and training program. In addition, international information security management and supply chain process integration and certification standards can assist in the development of an organization-wide program that includes training. International standards are listed in Appendix C of NISTIR 7622.

• **Use defensive design for systems, elements, and processes**. Defensive design techniques can aid in supply chain risk management. The techniques should be applied to supply chain elements, element processes, information, systems, and organizational processes throughout

the system or element life cycle. Defensive design techniques address contingencies in the technical, behavioral, and organizational activities that could result in adverse supply chain events. Defensive design creates options that preserve the integrity of the organization's mission and its performance to the end user or consumer of the supply chain element should any of the contingencies or contingency elements arise. Defensive design also increases flexibility for handling uncertainty and adapting to changing circumstances such as environmental, malicious, or unintentional harm within the supply chain, and can reduce the likelihood or consequences of attack.

• **Perform continuous integrator review**. Continuous integrator review includes testing, monitoring, auditing, assessments, and any other means by which the acquirer observes integrator practices. The review enables the acquirer to validate compliance with requirements, ascertain that the system behaves in a predictable manner under stress, and detect and classify weaknesses and vulnerabilities of elements, processes, systems, and any associated metadata. Federal department and agency acquirers should use the continuous integrator review to help determine if integrators are fulfilling the requirements defined in their agreements with integrators and whether any remedial actions are required based on the environment and use. Continuous integrator review should be conducted during the system or element life cycle including development, operations, sustainment, and disposal.

• **Strengthen delivery mechanisms**. Delivery includes inventory management, and can involve physical delivery of hardware as well as logical delivery of software modules and patches. Delivery may occur across a system or element life cycle, among multiple parties and multiple links of a given supply chain, and includes acquirers, multiple integrators, and multiple suppliers. Because delivery may be compromised anywhere along the supply chain and system or element life cycle, federal department and agency acquirers should ensure protection of both physical and logical element delivery mechanisms to adequately protect the confidentiality, integrity, or availability of systems and elements delivered through the supply chain.

• **Assure sustainment activities and processes**. The sustainment process begins when an element or a system becomes operational, and ends when it enters the disposal process. This includes system maintenance, upgrade, patching, element replacement and other activities that keep the system or element operational. Changes to the elements, system, or process can take place at any stage of the system or element life cycle, and can introduce opportunities for subversion throughout the supply chain. Sustainment processes should limit opportunities and means for compromise of the confidentiality, availability, and integrity of elements and operational processes. Federal department and agency acquirers should include provisions for safe processes in their agreements with their integrators, who are responsible for sustainment. See draft NIST SP 800-53 Rev.4 or later versions for security controls that should be used.

• **Manage disposal and final disposition activities throughout the system or element life cycle**. Elements, information, and data may be disposed of at any time in the system and element life cycle, including during R&D, design, prototyping, or operations and maintenance. Methods used include disk cleaning, removal of cryptographic keys, and partial reuse of components. Poor disposal procedures and undefined rules for disposal can lead to unauthorized access to, and compromise of, systems and elements. See NIST SP 800-88, *Guidelines for Media Sanitization,* for help in implementing a media sanitization program that applies techniques and controls for sanitization and for making disposal decisions.

**For More Information**

U.S. legislation and policies require federal departments and agencies to use international, voluntary consensus standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical. The ICT SCRM approach and practices described in this document are rooted in many current and emerging international standards as well as government and industry documents. See Appendix C of NISTIR 7622 for a complete list of references, including national and international standards, policies, and guides developed by federal government organizations, and NIST publications.

The supply chain risk management approach described in NISTIR 7622 is supported by NIST security standards and guidelines that have been issued for managing information security risk, including:

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
NIST Special Publication (SP) 800-30 Rev.1, *Guide for Conducting Risk Assessments*
NIST SP 800-37 Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems*: *A Security Life Cycle Approach*
NIST SP 800-40 Rev.2, *Creating a Patch and Vulnerability Management Program*
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
NIST Draft SP 800-53 Rev.4, *Recommended Security Controls for Federal Information Systems*. This publication is being revised to include security controls for supply chain protection.
NIST SP 800-61 Rev.2, *Computer Security Incident Handling Guide*
NIST SP 800-70 Rev.2, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*
NIST SP 800-88, *Guidelines for Media Sanitization*
NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
NISTSP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*

These publications are available here.


Information about NIST's information security programs is available from the Computer Security Resource Center here.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.