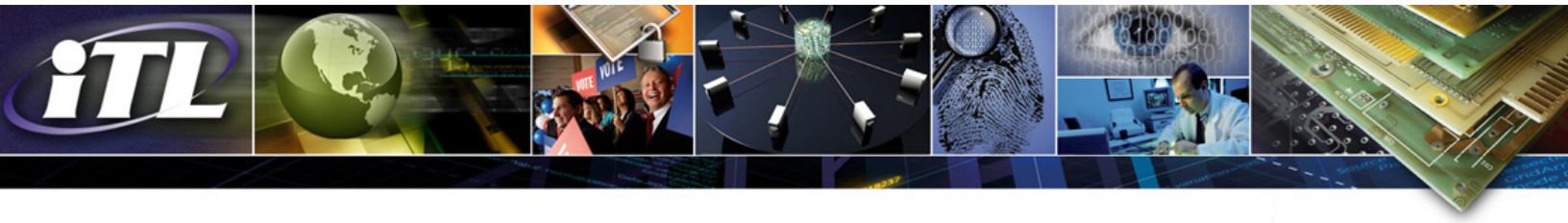


ITL BULLETIN FOR JUNE 2015
INCREASING VISIBILITY AND CONTROL OF YOUR ICT SUPPLY CHAINS

Jon Boyens, Celia Paulsen, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

Federal agencies rely on complex information and communications technology (ICT) that is developed and supported by a multifaceted and globally distributed network of suppliers, integrators, and service providers. Modern ICT supply chains are subject to a variety of risks. These risks may affect the confidentiality, integrity, or availability of government systems and include insertion of counterfeits, unauthorized production, tampering, theft, and insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain.

Without effective security processes and practices throughout the life cycle of a system, intentional and unintentional vulnerabilities can be placed into systems. The systems may then 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.

NIST has released a new publication, Special Publication (SP) 800-161, *Supply Chain Management Practices for Federal Information Systems and Organizations*, which provides guidance to federal agencies for identifying, assessing, and mitigating ICT supply chain risks. It builds on existing guidance and is focused on increasing agencies' visibility and control over the practices and procedures used to protect a system throughout its life cycle.

This publication represents several years of research and collaboration with industry, academic, and government stakeholders. It draws upon work started in 2008 as part of the Comprehensive National Cybersecurity Initiative number 11, which resulted in the publication of NIST Interagency Report (NISTIR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*. A collaborative ICT SCRM community workshop was hosted by NIST in October 2012 that provided consensus on the approach and methodology for moving forward in developing NIST SP 800-161.

The intended audience for this publication is federal agency personnel that support ICT components and systems through all system development life cycle (SDLC) activities, although other organizations and personnel are free to use the guidance as it applies to their situation.

Supply Chain Risk Management

ICT SCRM is a new discipline that is concerned about security, integrity, resilience, and quality of products, services, and the supply chain, as depicted in Figure 1, and can be said to lie at the intersection of these various specialties or risk areas.

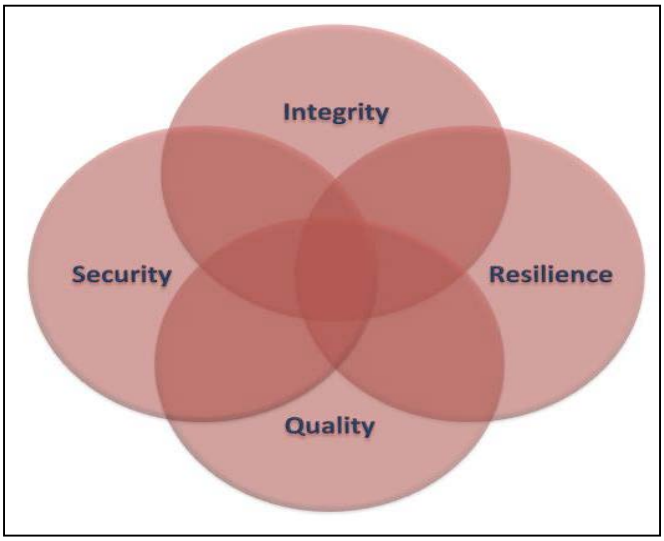
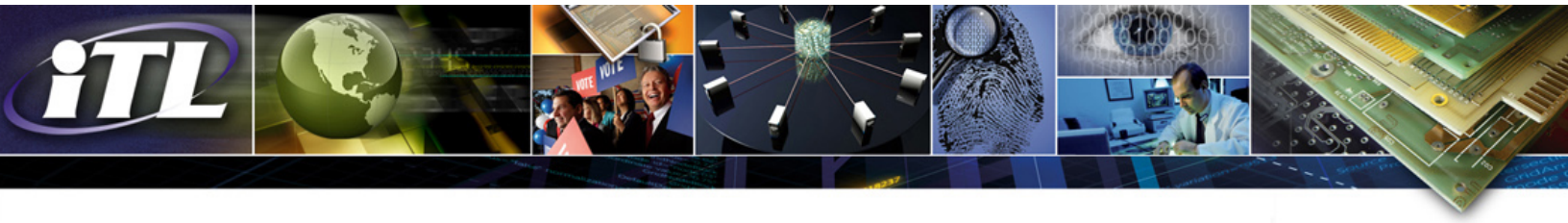


Figure 1: Four Pillars of ICT SCRM

- Security provides the confidentiality, integrity, and availability of information about the supply chain or products and services that traverse the supply chain;
- Integrity is focused on ensuring that the ICT products or services in the ICT supply chain are genuine and will perform according to acquirer specifications and without any unwanted functionality;
- Resilience is focused on ensuring that the ICT supply chain will be able to provide required ICT products and services under stress or failure; and
- Quality is focused on reducing vulnerabilities that may limit the intended function of a component, lead to component failure, or provide opportunities for exploitation.

For effectiveness of implementation, NIST SP 800-161 recommends that ICT SCRM should be integrated into the organization-wide risk management process described in NIST SP 800-39. This process includes the following continuous and iterative steps:

- Frame risk – establish the context for risk-based decisions and the current state of the information system or ICT supply chain infrastructure;
- Assess risk – review and interpret criticality, threat, vulnerability, likelihood, impact, and related information;



- Respond to risk once determined – select, tailor, and implement mitigation controls; and
- Monitor risk on an ongoing basis, including changes to an information system or ICT supply chain infrastructure, using effective organizational communications and a feedback loop for continuous improvement.

Recommended Practices

As described in NIST SP 800-53 Revision 4, an overlay provides a set of security controls, control enhancements, and supplemental guidance to address specialized requirements or environments. NIST SP 800-161 contains an overlay of the controls provided in NIST SP 800-53 Rev. 4; it identifies, refines, and expands ICT SCRM-related controls. This approach leverages the existing work of federal agencies as well as industry suppliers, integrators, and providers who use NIST SP 800-53A Rev. 4.

In addition, the document also provides a *new* control family titled "Provenance" and a total of four new controls to address ICT SCRM-specific concerns. The provenance control family involves the recording of the origin of, history of, and changes to components and systems. Creating and maintaining provenance within the ICT supply chain helps government agencies to achieve greater traceability in case of an adverse event and is critical for developing an understanding of - and mitigating strategy for – ICT supply chain risks.

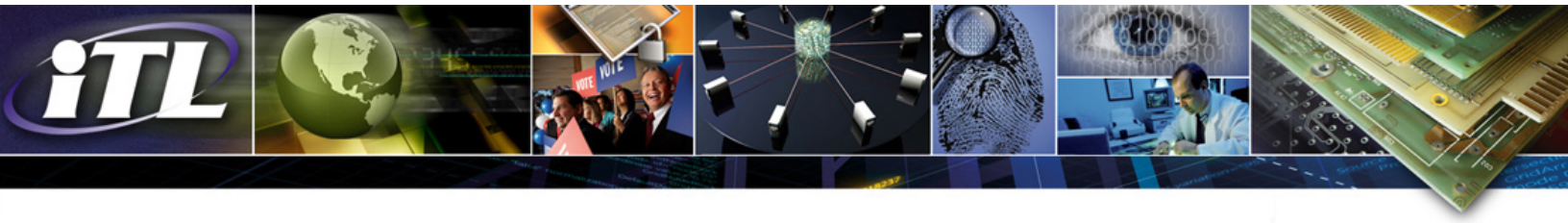
SCRM-specific supplemental guidance was provided to help organizations understand how the control relates or can be applied to ICT SCRM. In addition, the document specifies the tier(s) of the risk management process (organization, mission, system) to which each control applies, as described in NIST SP 800-39.

Although NIST SP 800-161 is intended for FIPS 199-defined "High" assurance systems, the ICT SCRM controls defined in this publication should be selected and tailored according to organizational needs and their environment, using the guidance in NIST SP 800-53 Rev. 4, to ensure a cost-effective, risk-based approach.

The publication strongly recommends that federal agencies work with suppliers to identify how their products and services meet the agency's ICT SCRM needs. Many suppliers will likely be willing to work with federal agencies to identify a mutually acceptable ICT SCRM strategy. However, requiring any practices that the supplier does not already provide as a part of their regular business processes may or may not be practical and could result in significant additional costs to the agency. Federal agencies should evaluate and weigh the costs of adding ICT SCRM requirements into agreements against the risks to the organization of not adding ICT SCRM requirements.

ICT SCRM Plan Template

NIST SP 800-161 provides a template as an example of the sections and the type of information that organizations should include in ICT SCRM plans. The publication defines guidance for specific tiers, where applicable.



Agencies should have at least one ICT SCRM plan. Depending on the governance structure and size, agencies can have multiple ICT SCRM plans, such as one for Tier 1, several for Tier 2, and several for Tier 3. Regardless of the total number of plans, the ICT SCRM requirements and controls at the higher tiers will flow down to the lower tiers and should be used to guide the development of the lower tier ICT SCRM plans. Conversely, the ICT SCRM controls and requirements at the lower tiers should be considered in developing and revising requirements and controls applied at the higher tiers.

ICT SCRM plans should cover the full SDLC of ICT systems and programs, including product and service acquisitions. The publication recommends integration of the ICT SCRM plan activities into the organization's system and software life cycle processes.

Conclusion

Risk from ICT supply chains is widely recognized as a principal concern for federal departments and agencies. This risk is seen as the cumulative effect of the growing sophistication of ICT, mounting scale of information systems, and growing speed and complexity of a distributed global supply chain. NIST SP 800-161 provides guidance to federal agencies, although many types of enterprises will benefit from the application of these processes and tools to integrate SCRM into the organization-wide risk management.

Additional Resources

NIST's ICT SCRM Program website: http://scrm.nist.gov/

Department of Homeland Security (DHS) Software and Supply Chain Assurance Forum: https://buildsecurityin.us-cert.gov/swa/

NIST-sponsored research at the University of Maryland: http://csrc.nist.gov/scrm/references.htmll#nistsponres

ITL Bulletin Publisher: Elizabeth B. Lennon

Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov