Information and Communications Technology Supply Chain Risk Management (ICT SCRM)

The National Institute of Standards and Technology (NIST) is responsible for developing standards, guidelines, tests, and metrics for the protection of non-national security federal information and communication infrastructure. Over the past several years, NIST has collaborated with public and private sector stakeholders to research and develop **Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)** tools and metrics, as well as guidelines on mitigation strategies and implementation methodologies.

Background

NIST's ICT SCRM program started in 2008, when it initiated the development of ICT SCRM practices for non-national security information systems, in response to **Comprehensive National Cybersecurity Initiative (CNCI) #11,** "Develop a multi-pronged approach for global supply chain risk management." NIST co-leads CNCI 11 Working Group 2, Life Cycle Processes and Standards, with the Department of Defense. Working Group 2 is responsible for developing supply chain tools, resources and risk management practices, in partnership with industry.

NIST has worked closely with diverse stakeholders from across academia, industry and government to develop a set of foundational, repeatable, and feasible practices—reflecting the complex global marketplace—to assist federal agencies in managing ICT supply chain risks to their information systems and organizations. NIST has issued four grants to study the state of ICT SCRM in private sector suppliers to the government, identify and analyze ICT SCRM strategies and initiatives, and develop a web-based risk assessment and collaboration tool. In October 2012, NIST published NIST Interagency Report (IR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, containing ICT SCRM methods and practices. NIST also held a two-day workshop to engage stakeholders on the fundamental underpinnings of ICT SCRM, including the identification of current and needed: commercially reasonable ICT SCRM standards and practices; tools, technologies and techniques; and research and resources. The workshop set a foundation for NIST's current work on ICT SCRM and provided direction for the development of draft NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

Approach

Organizations are increasingly at risk of supply chain compromise, whether intentional or unintentional. Managing ICT supply chain risk requires ensuring the integrity, security, and resilience of the supply chain and its products and services, with their quality also being ensured. NIST has developed an approach to ICT SCRM that encompasses the following key points:

- **Foundational Practices**: ICT SCRM lies at the intersection of information security and supply chain management. Existing supply chain and cybersecurity practices provide a foundation for building an effective ICT SCRM program.
- **Organization-wide**: Effective ICT SCRM is an organization-wide activity that involves each organizational tier (Organization, Mission/Business Processes, and Information Systems) and is implemented throughout the system development life cycle.
- **Risk Management Process**: ICT SCRM should be implemented as part of overall risk management activities, such as those described in NIST SP 800-39, *Managing Information Security Risk*. 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 that Plan. Because ICT supply chains differ across and within organizations, the ICT SCRM Plan should be tailored to individual organizational contexts.
    - **Risk**: ICT supply chain risk is associated with a lack of visibility into, understanding of, and control over many of the processes and decisions involved in the development and delivery of ICT products and services acquired by federal agencies.

- **Threats and Vulnerabilities**: Effectively managing ICT supply chain risks requires a comprehensive view of threats and vulnerabilities. Threats can be either "adversarial" (e.g. tampering, counterfeits) or "non-adversarial" (e.g. poor quality, natural disasters); vulnerabilities may be "internal" (e.g. organizational procedures) or "external" (e.g. part of an organization's supply chain).

- **Critical Systems**: Cost-effective supply chain risk mitigation requires agencies to identify those systems/components that are most vulnerable and will cause the largest organizational impact if compromised.

Key Resources for Federal Agencies

CNCI 11: CNCI 11 provides U.S. federal agencies with a holistic, multipronged approach for managing supply chain risk at a level commensurate with the criticality of information systems or networks. CNCI 11 WG2 facilitates SCRM by: offering greater awareness of threats, vulnerabilities, and consequences associated with acquisition decisions; developing collaboration tools; and identifying resources for mitigating risk across the life cycle of products and services.

Draft* NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations: NIST SP 800-161 provides federal agencies with guidance to develop the appropriate policies, processes, and controls to effectively manage ICT supply chain risk. It is flexible and builds on agencies' existing information security practices.

- **Risk Management**: NIST SP 800-161 details a set of processes for evaluating and managing supply chain risk. These processes are integrated into the NIST SP 800-39's Risk Management Process (Frame, Assess, Respond, and Monitor) and should be implemented as part of agencies' overall risk management activities.
- **Extended Overlay:** Several controls in Appendix F of NIST SP 800-53 Rev. 4 can help with ICT supply chain risk mitigation. Chapter 3 of NIST SP 800-161 identifies these controls and provides supplementary guidance for their application to ICT SCRM. Additional controls assist organizations in developing more robust and complete ICT SCRM mitigation strategies.
- **Threat Scenarios and Risk Framework:** Understanding and evaluating ICT SCRM threats supports a cost-effective risk mitigation strategy. NIST SP 800-161 lists applicable threat events and provides a risk framework for assessing threats and identifying mitigation responses—one method for evaluating interdependencies and the potential impact of an event.
- **ICT SCRM Plan:** NIST SP 800-161 provides a template for developing ICT SCRM plans that address the entire system development life cycle.

Additional Resources:

- **NIST's ICT SCRM Program website:** http://scrm.nist.gov
- **NIST ICT SCRM Workshop Summary:** http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913338
- **DHS Software and Supply Chain Assurance:** https://buildsecurityin.us-cert.gov/swa
- **UMD Research**: http://csrc.nist.gov/scrm/publications.html
- **ISO/IEC 27036:** *Information Security for Supplier Relationships (Four Parts*). Part 1 is free: http://standards.iso.org/ittf/PubliclyAvailableStandards/c059648_ISO_IEC_27036-1_2014.zip; Part 3: http://www.iso.org/iso/catalogue_detail.htm?csnumber=59688
- **SAFECode:** http://www.safecode.org/index.php
- **The Open Group Trusted Technology Forum:** http://www.opengroup.org/ottf/
- **SAE International standards ARP9113,** *Supply Chain Risk Management Guidelines***, and AS5553,** *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition***:** http://www.sae.org/

For more information contact: Jon Boyens, NIST, 301-975-5549 (T), Boyens@nist.gov