Cyber Supply Chain Risk Management
(C-SCRM)

The National Institute of Standards and Technology (NIST) is responsible for developing reliable and practical standards, guidelines, tests, and metrics to help protect non-national security federal information and communications infrastructure. The private sector and other government organizations also rely heavily on these NIST-produced resources. That includes organizations developing or using information, communications, and operational technologies which depend upon complex, globally distributed, and interconnected supply chains. These supply chains cover the entire life cycle—from research and development, design, and manufacturing to acquisition, delivery, integration, operations and maintenance, and disposal.

NIST conducts research and collaborates with a large number and variety of stakeholders to produce information resources which help organizations with their **Cyber Supply Chain Risk Management – or C-SCRM.** By statute, federal agencies must use NIST's C-SCRM and other cybersecurity standards and guidelines to protect non-national security federal information and communications infrastructure. The SECURE Technology Act and FASC Interim Final Rule gave NIST specific authority to develop C-SCRM guidelines. NIST is also a member of the Federal Acquisition Security Council (FASC).

Scope and Approach

Managing cyber supply chain risk requires ensuring the integrity, security, quality, and resilience of the supply chain and its products and services. NIST focuses on:

- **Foundational practices**: C-SCRM lies at the intersection of information security and supply chain risk management. Existing supply chain and cybersecurity practices provide a foundation for building an effective risk management program.
- **Enterprise-wide practices**: Effective C-SCRM is an enterprise-wide activity that involves each tier (Organization, Mission and Business Processes, and Information Systems) and is implemented throughout the system development life cycle.
- **Risk management processes**: C-SCRM should be implemented as part of overall risk management activities, such as those described in *Managing Information Security Risk (*NIST SP 800-39*), the NIST Framework for Improving Critical Infrastructure (the Cybersecurity Framework),* and *Integrating Cybersecurity and Enterprise Rick Management (NISTIR 8286)*. Activities should involve identifying and assessing applicable risks, determining appropriate response actions, developing a C-SCRM Strategy and Implementation Plan to document selected response actions, and monitoring performance against that Plan. Because cyber supply chains differ across and within organizations, the Strategy and Plan should be tailored to individual organizational contexts.

    - **Risk**: Cyber 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 cyber products and services acquired by federal agencies.
    - **Threats and Vulnerabilities**: Effectively managing cyber 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 organizations to identify those systems and components that are most vulnerable and will cause the largest organizational impact if compromised.

Key NIST Resources and Activities

Focusing on federal agencies but also engaging with and providing resources useful to government at other levels as well as the private sector, NIST:

- Produced "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*" (SP 800-161) in 2015, which guides organizations in identifying, assessing, and responding to supply chain risks at all levels of their organizations. It is flexible and builds on organizations' existing information security practices. NIST expects to revise this primary technical resource in 2021.
- Participates in the Federal Acquisition Security Council, or FASC, created by statute in 2018. The Council helps to develop policies and processes for agencies to use when purchasing technology products and services. It recommends C-SCRM standards, guidelines, and practices that NIST should develop**.**
- Integrated C-SCRM considerations into other NIST guidance, including the *Cybersecurity Framework*, *Risk Management Framework*, and *Security and Privacy Controls for Information Systems and Organizations (SP 800-53R5)* – all widely used by federal agencies and others.
- Issued *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks (NISTIR 8272)*, which describes a prototype solution for filling the gap between an organization's risk appetite and supply chain risk posture by providing a basic measurement of the potential impact on a cyber supply chain.
- Released *Criticality Analysis Process Model: Prioritizing Systems and Components (NISTIR 8179),* aimed at identifying systems and components that are most vital and may need additional security or other protections.
- Drafted *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (NISTIR 8276),* summarizing practices found to be foundational to an effective cyber supply chain risk management program. NIST expects to finalize this publication by March 2021.
- Hosts the Federal C-SCRM Forum, which fosters collaboration and the exchange of information among federal organizations to improve the security of their supply chains. It includes those responsible for C-

SCRM in the federal ecosystem, among them the Office of Management and Budget (OMB), Department of Defense (DOD), Office of the Director for National Intelligence (ODNI), Cybersecurity and Infrastructure Security Agency (CISA), General Services Administration (GSA), and NIST.

- Co-leads the Software and Supply Chain Assurance (SSCA) Forum with DOD, DHS, and GSA. The SSCA Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.
- Is organizing a demonstration project to identify methods by which organizations can verify that their purchased computing devices' internal components are genuine and have not been altered during the manufacturing and distribution processes or after sale from a retailer until the device is retired from service. This project is a collaboration with the private sector via the NIST-led National Cybersecurity Center of Excellence (NCCoE), which is also developing guidance on challenges and benefits of using various blockchain technologies for manufacturing supply chain traceability.

Additional Resources:

- **NIST's C-SCRM Program website:** http://scrm.nist.gov
- **NIST's Case Studies and Key Practices in C-SCRM Project:** https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/key-practices
- **NIST's Supply Chain Interdependency Tool:** https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/interdependency-tool
- **NIST-sponsored Research on C-SCRM:** https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/NIST-Sponsored-Research
- **Software and Supply Chain Assurance Forum:** https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca
- **Federal C-SCRM Forum:** https://csrc.nist.gov/federal-c-scrm

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

February 2021