NIST CYBERSECURITY & PRIVACY PROGRAM

Cybersecurity Supply Chain Risk Management

When a supply chain is compromised, its security can no longer be trusted, whether it involves a chip, laptop, server, other technology, a non-electronic product, or a service. The National Institute of Standards and Technology (NIST) is responsible for developing reliable and practical standards, guidelines, tests, and metrics to help manufacturers, retailers, government agencies, and other organizations with their Cybersecurity Supply Chain Risk Management (C-SCRM). The private and public sectors rely heavily on these NIST-produced resources. That includes organizations that develop – or simply use – information, communications, and operational technologies that depend upon complex, globally distributed, and interconnected supply chains. These supply chains cover the lifecycle – from research and development, design, and manufacturing to acquisition, delivery, integration, operations and maintenance, and disposal.

NIST has collaborated with public and private sector stakeholders to research and develop C-SCRM tools and metrics, producing case studies and widely used guidelines on mitigation strategies. These multiple resources reflect the complex global marketplace and assist federal agencies, companies, and others in managing cybersecurity risks in supply chains that threaten their information systems and organizations. The SECURE Technology Act and FASC Final Rule gave NIST specific authority to develop C-SCRM guidelines. NIST is also a member of the Federal Acquisition Security Council (FASC). A May 2021 Executive Order assigned NIST additional responsibilities related to software supply chains relied upon by federal agencies.

SCOPE AND APPROACH

Managing cybersecurity 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 Cybersecurity Framework, and *Integrating Cybersecurity and Enterprise Rick Management (NISTIR 8286)*. Activities should involve identifying and assessing applicable risks, determining appropriate responses, developing a C-SCRM Strategy and Implementation Plan to document selected responses, 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 processes and decisions involved in developing and delivering cyber products and services acquired by federal agencies.
    - **Threats and Vulnerabilities**: Effectively managing cyber supply chain risk 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 systems and components that are most vulnerable and cause the largest organizational impact if compromised.

KEY NIST RESOURCES & ACTIVITIES

Focusing on federal agencies – while also engaging with and providing resources useful to other levels of government and the private sector – NIST:

- Produced *Cybersecurity Supply Chain Risk Management for Systems and Organizations (SP 800-161 Revision 1)* to guide organizations in identifying, assessing, and responding to supply chain risks at all levels. It is flexible and builds on organizations' existing information security practices.
- Participates in the Federal Acquisition Security Council, or FASC, created by law 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 800-53 R5)* – all widely used by federal agencies and others.
- 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.
- Released *Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives (NISTIR 8419)*, which explores the issues that surround traceability, the role that blockchain and related technologies may be able to play to improve traceability, and several industry case studies.
- Finalized *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (NISTIR 8276)*, summarizing practices foundational to an effective C-SCRM program.
- 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 Forum with DOD, the Department of Homeland Security (DHS), and GSA. The 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.
- Released Preliminary Draft NIST Cybersecurity Practice Guide 1800-34, *Validating the Integrity of Computing Devices* (Volumes A, B, and C), which is a multi-year culmination of a demonstration project to identify methods to help organizations verify that their purchased computing devices' internal components are genuine and have not been altered during manufacturing or distribution or after sale from a retailer until the device is retired from service. This is a collaboration with the private sector via the NIST-led National Cybersecurity Center of Excellence (NCCoE).

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-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 at NIST:
301-975-5549 (T) | Boyens@NIST.gov