https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management

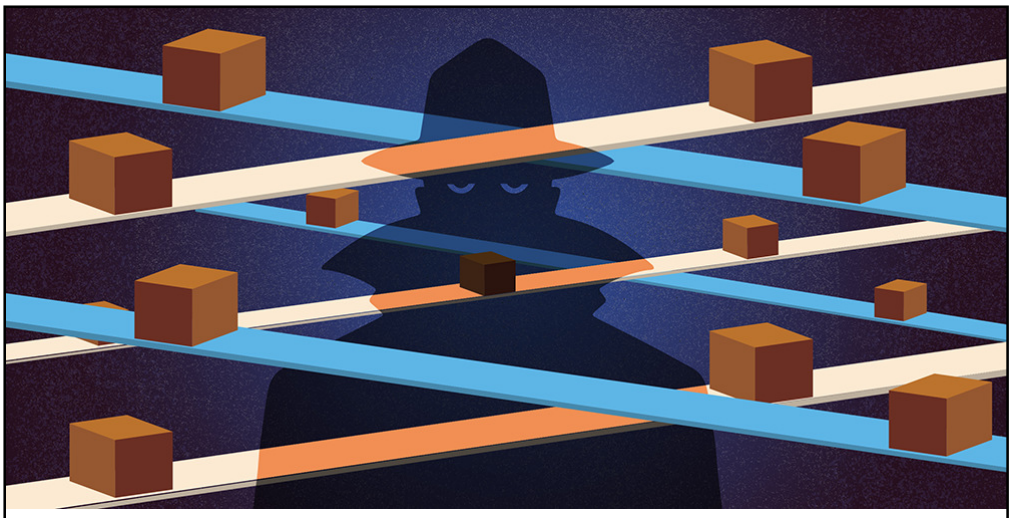
National Institute of Standards and Technology
U.S. Department of Commerce

NEWS (https://www.nist.gov/news-events/news)

NIST Updates Cybersecurity Guidance for Supply Chain Risk Management

The publication's revisions form part of NIST's response to an executive order regarding cybersecurity.

May 05, 2022



The global supply chain places companies and consumers at cybersecurity risk because of the many sources of components and software that often compose a finished product: A device may have been designed in one country and built in another using multiple components manufactured in various parts of the world.
Credit: B. Hayes/NIST

A vulnerable spot in global commerce is the supply chain: It enables technology developers and vendors to create and deliver innovative products but can leave businesses, their finished wares, and ultimately their consumers open to cyberattacks. A new update to the National Institute of Standards and Technology's (NIST's) foundational cybersecurity supply chain risk management (C-SCRM) guidance aims

to help organizations protect themselves as they acquire and use technology products and services.

The revised publication, formally titled *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST Special Publication 800-161 Revision 1 (https://doi.org/10.6028/NIST.SP.800-161r1)), provides guidance on identifying, assessing and responding to cybersecurity risks throughout the supply chain at all levels of an organization. It forms part of NIST's response (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity) to Executive Order 14028 (https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity): *Improving the Nation's Cybersecurity,* specifically Sections 4(c) and (d) (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains), which concern enhancing the security of the software supply chain.

Released today after a multiyear development process that included two draft versions (https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft), the publication now offers key practices for organizations to adopt as they develop their capability to manage cybersecurity risks within and across their supply chains. It encourages organizations to consider the vulnerabilities not only of a finished product they are considering using, but also of its components — which may have been developed elsewhere — and the journey those components took to reach their destination.

"Managing the cybersecurity of the supply chain is a need that is here to stay," said NIST's Jon Boyens, one of the publication's authors. "If your agency or organization hasn't started on it, this is a comprehensive tool that can take you from crawl to walk to run, and it can help you do so immediately."

Modern products and services depend on their supply chains, which connect a worldwide network of manufacturers, software developers and other service providers. Though they enable the global economy, supply chains also place companies and consumers at risk because of the many sources of components and software that often compose a finished product: A device may have been designed in one country and built in another using multiple components from various parts of the world that have themselves been assembled of parts from disparate manufacturers. Not only might the resulting product contain malicious software or be susceptible to cyberattack, but the vulnerability of the supply chain itself can affect a company's bottom line.

"A manufacturer might experience a supply disruption for critical manufacturing components due to a ransomware attack at one of its suppliers, or a retail chain might experience a data breach because the company that maintains its air conditioning systems has access to the store's data sharing portal," Boyens said.

The primary audience for the revised publication is acquirers and end users of products, software and services. The guidance helps organizations build cybersecurity supply chain risk considerations and requirements into their acquisition processes and highlights the importance of monitoring for risks. Because cybersecurity risks can arise at any point in the life cycle or any link in the supply chain, the guidance now considers potential vulnerabilities such as the sources of code within a product, for example, or retailers that carry it.

"If your agency or organization hasn't started on [C-SCRM], this is a comprehensive tool that can take you from crawl to walk to run, and it can help you do so immediately." —NIST's Jon Boyens

"It has to do with trust and confidence," said NIST's Angela Smith, an information security specialist and another of the publication's authors. "Organizations need to have greater assurance that what they are purchasing and using is trustworthy. This new guidance can help you understand what risks to look for and what actions to consider taking in response."

Before providing specific guidance — called cybersecurity controls, which are listed in Appendix A — the publication offers help to the varied groups in its intended audience, which ranges from cybersecurity specialists and risk managers to systems engineers and procurement officials. Each group is offered a "user profile" in Section 1.4, which advises what parts of the publication are most relevant to the group.

The publication's Sections 1.6 and 1.7 specify how it integrates guidance promoted within other NIST publications and tailors that guidance for C-SCRM. These other publications include NIST's Cybersecurity Framework (https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework) and Risk Management Framework (https://www.nist.gov/news-events/news/2018/05/nist-updates-risk-management-framework-incorporate-privacy-considerations), as well as *Security and Privacy Controls for Information Systems and Organizations (https://www.nist.gov/news-events/news/2020/03/nist-updates-and-expands-its-flagship-catalog-information-system-safeguards)*, or SP 800-53 Rev. 5, its flagship catalog of information system safeguards. Organizations that are already using SP 800-53 Rev. 5's safeguards may find useful perspective in Appendix B, which details how SP 800-161 Rev. 1's cybersecurity controls map onto them.

Organizations seeking to implement C-SCRM in accordance with Executive Order 14028 should visit NIST's dedicated web-based portal (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity), as Appendix F now indicates. This information has been moved online, in part to reflect evolving guidance without directly affecting the published version of SP 800-161 Rev. 1.

In part because of the complexity of the subject, the authors are planning a quick-start guide to help readers who may be just beginning their organization's C-SCRM effort. Boyens said they also plan to offer the main publication as a user-friendly webpage.

"We plan to augment the document's current PDF format with a clickable web version," he said. "Depending on what group of users you fall into, it will allow you to click on a link and find the sections you need."

The publication is available on the NIST website (https://doi.org/10.6028/NIST.SP.800-161r1).

Information technology (https://www.nist.gov/topic-terms/information-technology), Cybersecurity (https://www.nist.gov/topic-terms/cybersecurity) and Risk management (https://www.nist.gov/topic-terms/risk-management)

Media Contact

- Chad Boutin (https://www.nist.gov/people/chad-boutin)
  charles.boutin@nist.gov (https://www.nist.govmailto:charles.boutin@nist.gov)
  (301) 975-4261

Related Links

NIST SP 800-161 Rev. 1 (https://doi.org/10.6028/NIST.SP.800-161r1)
Released May 5, 2022