NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

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

NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
Boston Consulting Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

May 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-161r1
Natl. Inst. Stand. Technol. Spec. Publ. 800-161r1, 326 pages (May 2022)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

Submit comments on this publication to: scrm-nist@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services.

This publication provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. The publication integrates cybersecurity supply chain risk management (C-SCRM) into risk management activities by applying a multilevel, C-SCRM-specific approach, including guidance on the development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and risk assessments for products and services.

Keywords

acquire; C-SCRM; cybersecurity supply chain; cybersecurity supply chain risk management; information and communication technology; risk management; supplier; supply chain; supply chain risk assessment; supply chain assurance; supply chain risk; supply chain security.

Acknowledgments

The authors – Jon Boyens of the National Institute of Standards and Technology (NIST), Angela Smith (NIST), Nadya Bartol, Boston Consulting Group (BCG), Kris Winkler (BCG), Alex Holbrook (BCG), and Matthew Fallon (BCG) – would like to acknowledge and thank Alexander Nelson (NIST), Murugiah Souppaya (NIST), Paul Black (NIST), Victoria Pillitteri (NIST), Kevin Stine (NIST), Stephen Quinn (NIST), Nahla Ivy (NIST), Isabel Van Wyk (NIST), Jim Foti (NIST), Matthew Barrett (Cyber ESI), Greg Witte (Huntington Ingalls), R.K. Gardner (New World Technology Partners), David A. Wheeler (Linux Foundation), Karen Scarfone (Scarfone Cybersecurity), Natalie Lehr-Lopez (ODNI/NCSC), Halley Farrell (BCG), and the original authors of NIST SP 800-161, Celia Paulsen (NIST), Rama Moorthy (Hatha Systems), and Stephanie Shankles (U.S. Department of Veterans Affairs) for their contributions. The authors would also like to thank the C-SCRM community, which has provided invaluable insight and diverse perspectives for managing the supply chain, especially the departments and agencies who shared their experience and documentation on NIST SP 800-161 implementation since its release in 2015, as well as the public and private members of the Enduring Security Framework who collaborated to provide input to Appendix F.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Figures

List of Tables