

**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>

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

**NIST Special Publication
NIST SP 800-161r1**

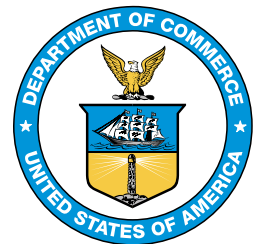
Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

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>

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

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

All comments are subject to release under the Freedom of Information Act (FOIA).

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

1. INTRODUCTION..... 1

1.1. Purpose 4

1.2. Target Audience 4

1.3. Guidance for Cloud Service Providers 5

1.4. Audience Profiles and Document Use Guidance 5

1.4.1. Enterprise Risk Management and C-SCRM Owners and Operators..... 5

1.4.2. Enterprise, Agency, and Mission and Business Process Owners and Operators 5

1.4.3. Acquisition and Procurement Owners and Operators 6

1.4.4. Information Security, Privacy, or Cybersecurity Operators..... 6

1.4.5. System Development, System Engineering, and System Implementation Personnel..... 7

1.5. Background 7

1.5.1. Enterprise’s Supply Chain..... 9

1.5.2. Supplier Relationships Within Enterprises 10

1.6. Methodology for Building C-SCRM Guidance Using NIST SP 800-39; NIST SP 800-37, Rev 2; and NIST SP 800-53, Rev 5..... 13

1.7. Relationship to Other Publications and Publication Summary 14

2. INTEGRATION OF C-SCRM INTO ENTERPRISE-WIDE RISK MANAGEMENT 18

2.1. The Business Case for C-SCRM..... 19

2.2. Cybersecurity Risks Throughout Supply Chains 20

2.3. Multilevel Risk Management 22

2.3.1. Roles and Responsibilities Across the Three Levels..... 23

2.3.2. Level 1 – Enterprise 27

2.3.3. Level 2 – Mission and Business Process..... 30

2.3.4. Level 3 – Operational..... 32

2.3.5. C-SCRM PMO 34

3. CRITICAL SUCCESS FACTORS..... 37

3.1. C-SCRM in Acquisition 37

3.1.1. Acquisition in the C-SCRM Strategy and Implementation Plan..... 38

3.1.2. The Role of C-SCRM in the Acquisition Process..... 39

3.2. Supply Chain Information Sharing..... 43

3.3. C-SCRM Training and Awareness..... 45

3.4. C-SCRM Key Practices..... 46

3.4.1. Foundational Practices 47

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

3.4.2. Sustaining Practices 48

3.4.3. Enhancing Practices 49

3.5. Capability Implementation Measurement and C-SCRM Measures 49

3.5.1. Measuring C-SCRM Through Performance Measures 52

3.6. Dedicated Resources 54

REFERENCES..... 58

APPENDIX A: C-SCRM SECURITY CONTROLS 64

C-SCRM CONTROLS INTRODUCTION 64

C-SCRM CONTROLS SUMMARY..... 64

C-SCRM CONTROLS THROUGHOUT THE ENTERPRISE 65

APPLYING C-SCRM CONTROLS TO ACQUIRING PRODUCTS AND SERVICES..... 65

SELECTING, TAILORING, AND IMPLEMENTING C-SCRM SECURITY CONTROLS ... 68

C-SCRM SECURITY CONTROLS..... 71

FAMILY: ACCESS CONTROL 71

FAMILY: AWARENESS AND TRAINING..... 77

FAMILY: AUDIT AND ACCOUNTABILITY 80

FAMILY: ASSESSMENT, AUTHORIZATION, AND MONITORING 84

FAMILY: CONFIGURATION MANAGEMENT 87

FAMILY: CONTINGENCY PLANNING 97

FAMILY: IDENTIFICATION AND AUTHENTICATION 101

FAMILY: INCIDENT RESPONSE 104

FAMILY: MAINTENANCE..... 109

FAMILY: MEDIA PROTECTION 113

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION..... 115

FAMILY: PLANNING..... 119

FAMILY: PROGRAM MANAGEMENT 122

FAMILY: PERSONNEL SECURITY 128

FAMILY: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND
TRANSPARENCY..... 130

FAMILY: RISK ASSESSMENT 131

FAMILY: SYSTEM AND SERVICES ACQUISITION 134

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION..... 143

FAMILY: SYSTEM AND INFORMATION INTEGRITY 149

FAMILY: SUPPLY CHAIN RISK MANAGEMENT..... 153

APPENDIX B: C-SCRM CONTROL SUMMARY..... 158

APPENDIX C: RISK EXPOSURE FRAMEWORK..... 166

SAMPLE SCENARIOS..... 171

 SCENARIO 1: Influence or Control by Foreign Governments Over Suppliers..... 171

 SCENARIO 2: Telecommunications Counterfeits 176

 SCENARIO 3: Industrial Espionage 180

 SCENARIO 4: Malicious Code Insertion..... 185

 SCENARIO 5: Unintentional Compromise..... 188

 SCENARIO 6: Vulnerable Reused Components Within Systems 192

APPENDIX D: C-SCRM TEMPLATES 196

 1. C-SCRM STRATEGY AND IMPLEMENTATION PLAN 196

 1.1. C-SCRM Strategy and Implementation Plan Template..... 196

 2. C-SCRM POLICY 203

 2.1. C-SCRM Policy Template..... 203

 3. C-SCRM PLAN 208

 3.1. C-SCRM Plan Template..... 208

 4. CYBERSECURITY SUPPLY CHAIN RISK ASSESSMENT TEMPLATE 218

 4.1. C-SCRM Template..... 218

APPENDIX E: FASCSA 233

 INTRODUCTION 233

 Purpose, Audience, and Background 233

 Scope..... 233

 Relationship to NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* 234

 SUPPLY CHAIN RISK ASSESSMENTS (SCRAs) 235

 General Information..... 235

 Baseline Risk Factors (Common, Minimal) 236

 Risk Severity Schema 246

 Risk Response Guidance 247

 ASSESSMENT DOCUMENTATION AND RECORDS MANAGEMENT 249

 Content Documentation Guidance..... 249

 Assessment Record..... 251

APPENDIX F: RESPONSE TO EXECUTIVE ORDER 14028’s CALL TO PUBLISH GUIDELINES FOR ENHANCING SOFTWARE SUPPLY CHAIN SECURITY 252

APPENDIX G: C-SCRM ACTIVITIES IN THE RISK MANAGEMENT PROCESS 253

 TARGET AUDIENCE 255

 ENTERPRISE-WIDE RISK MANAGEMENT AND THE RMF 255

 Frame 255

Assess 277

Respond 287

Monitor 293

APPENDIX H: GLOSSARY 298

APPENDIX I: ACRONYMS 307

APPENDIX J: RESOURCES 313

RELATIONSHIP TO OTHER PROGRAMS AND PUBLICATIONS..... 313

 NIST Publications..... 313

 Regulatory and Legislative Guidance 314

 Other U.S. Government Reports..... 315

 Standards, Guidelines, and Best Practices 315

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

List of Figures

Fig. 1-1: Dimensions of C-SCRM	8
Fig. 1-2: An Enterprise’s Visibility, Understanding, and Control of its Supply Chain	11
Fig. 2-1: Risk Management Process	18
Fig. 2-2: Cybersecurity Risks Throughout the Supply Chain	21
Fig. 2-3: Multilevel Enterprise-Wide Risk Management	22
Fig. 2-4: C-SCRM Documents in Multilevel Enterprise-wide Risk Management	23
Fig. 2-5: Relationship Between C-SCRM Documents	27
Fig. 3-1: C-SCRM Metrics Development Process	52
Fig. A-1: C-SCRM Security Controls in NIST SP 800-161, Rev. 1	65
Fig. D-1: Example C-SCRM Plan Life Cycle	217
Fig. D-2: Example Likelihood Determination	230
Fig. D-3: Example Risk Exposure Determination	230
Fig. G-1: Cybersecurity Supply Chain Risk Management (C-SCRM)	253
Fig. G-2: C-SCRM Activities in the Risk Management Process	254
Fig. G-3: C-SCRM in the Frame Step	257
Fig. G-4: Risk Appetite and Risk Tolerance	274
Fig. G-5: Risk Appetite and Risk Tolerance Review Process	275
Fig. G-6: C-SCRM in the Assess Step	279
Fig. G-7: C-SCRM in the Respond Step	288
Fig. G-8: C-SCRM in the Monitor Step	295

List of Tables

Table 2-1: Cybersecurity Supply Chain Risk Management Stakeholders	24
Table 3-1: C-SCRM in the Procurement Process	41
Table 3-2: Supply Chain Characteristics and Cybersecurity Risk Factors Associated with a Product, Service, or Source of Supply	44
Table 3-3: Example C-SCRM Practice Implementation Model	51
Table 3-4: Example Measurement Topics Across the Risk Management Levels	53
Table A-1: C-SCRM Control Format	69
Table B-1: C-SCRM Control Summary	158
Table C-1: Sample Risk Exposure Framework	169
Table C-2: Scenario 1	173
Table C-3: Scenario 2	178
Table C-4: Scenario 3	182
Table C-5: Scenario 4	186
Table C-6: Scenario 5	189
Table C-6: Scenario 6	193
Table D-1: Objective 1 – Implementation milestones to effectively manage cybersecurity risks throughout the supply chain	199
Table D-2: Objective 2 – Implementation milestones for serving as a trusted source of supply for customers	200

Table D-3: Objective 3 – Implementation milestones to position the enterprise as an industry leader in C-SCRM	201
Table D-4: Version Management Table	202
Table D-5: Version Management Table	208
Table D-6: System Information Type and Categorization	210
Table D-7: Security Impact Categorization	210
Table D-8: System Operational Status	211
Table D-9: Information Exchange and System Connections	212
Table D-10: Role Identification	214
Table D-11: Revision and Maintenance	216
Table D-12: Acronym List	216
Table D-13: Information Gathering and Scoping Analysis	220
Table D-14: Version Management Table	232
Table E-1: Baseline Risk Factors	238
Table E-2: Risk Severity Schema	247
Table E-3: Assessment Record – Minimal Scope of Content and Documentation	250
Table G-1: Examples of Supply Chain Cybersecurity Threat Sources and Agents	261
Table G-2: Supply Chain Cybersecurity Threat Considerations	264
Table G-3: Supply Chain Cybersecurity Vulnerability Considerations	266
Table G-4: Supply Chain Cybersecurity Consequence and Impact Considerations	268
Table G-5: Supply Chain Cybersecurity Likelihood Considerations	270
Table G-6: Supply Chain Constraints	271
Table G-7: Supply Chain Risk Appetite and Risk Tolerance	275
Table G-8: Examples of Supply Chain Cybersecurity Vulnerabilities Mapped to the Enterprise Levels	283
Table G-9: Controls at Levels 1, 2, and 3	292