NIST Small Business Cybersecurity Quarterly Community of Interest Call

June 10, 2026
2:00 p.m. – 3:00 p.m. EDT

Daniel Eliot
Lead for Small Business Engagement
NIST

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

This call is not being recorded

Place into the chat if you feel comfortable doing so:

- Name
- Title
- Organization
- If you're a small business owner, employee, ecosystem partner, managed services provider, etc.

- NIST SMB Program Update
- NIST Pubs Seeking Comment
- Guest Speaker: Laura Calloway, Ph.D., Security Engineering and Risk Management Group
- Upcoming SMB Resources
- Next Call
- Open Discussion

NIST SMB Cybersecurity COI

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Convening companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work and assist NIST ***to better meet the cybersecurity needs of small businesses****.*

Over 21,000
individuals have already joined the full COI since March 6, 2023.

Quarterly meetings
to share resources, updates, host guest speakers, and have robust discussion.

Next Meeting:

September 16

nist.gov/itl/smallbusinesscyber/join-community-interest

NIST SMB Cybersecurity Resources

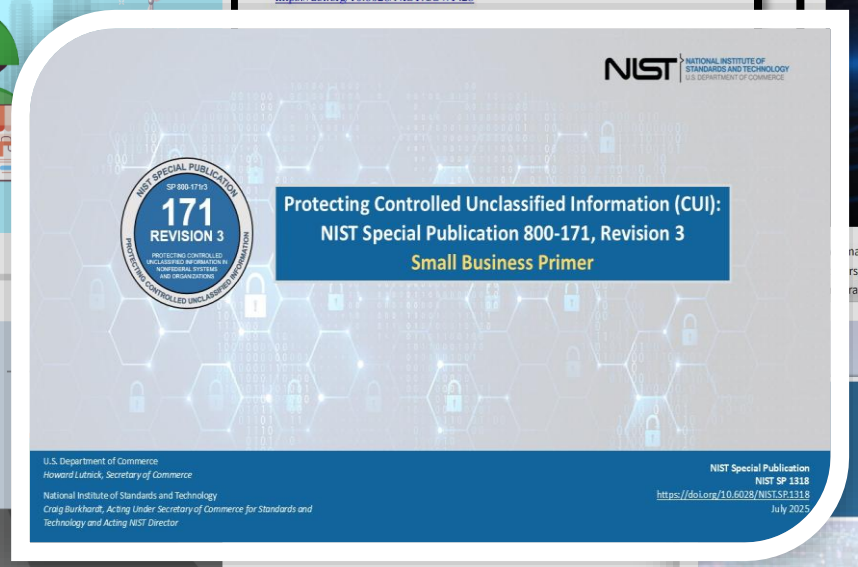
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Quick Start Guides
- Events
- Guidance by Sector +
- Guidance by Topic +
- Training +
- Videos
- Get Engaged +
- Cybersecurity @ NIST

CONNECT WITH US

SPOTLIGHT



www.nist.gov/itl/smallbusinesscyber

Recent NIST SMB Cybersecurity Updates

- **May 4 blog post**, "Stronger Cybersecurity, Stronger Business: NIST Celebrates 2026 National Small Business Week"

- **May 5 NIST Small Business Cybersecurity Webinar**: "Building Your Small Business Cybersecurity Team: From In-House to Outsourcing." Recording and slides available.

- **May 14 comment period closed** for CSWP 50, *Small Business Cybersecurity: Non-Employer Firms*

- **June 2 conference presentation:** 2026 NICE Conference & Expo

Let Your Voice Be Heard

Featured Open NIST Comment Period

NIST Special Publication 1800-41, *Responding to and Recovering from a Cyber Attack: Cybersecurity for the Manufacturing Sector*

https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack

Review the publication and share your feedback by July 8, 2026

For an exhaustive list of publications open for public comment, visit:
https://csrc.nist.gov/publications/drafts-open-for-comment

Guest Speaker: Laura Calloway, Ph.D., Security Engineering and Risk Management Group, NIST

Topic: Cybersecurity Supply Chain Risk Management

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Introduction to Cybersecurity Supply Chain Risk Management (C-SCRM)

Laura Calloway

June 2026

Cybersecurity Supply Chain Risk Management (C-SCRM) [at NIST]

Lead: *Research and Guidance for Organizations*
- Standalone (e.g., SP 800-161r1, NISTIR 8276, NISTIR 8179)
- Integrated (e.g., SPs 800-37r2, 53r5, CSF, IoT)

Advise: *Guidance for Technology Development*
- Software Assurance (e.g., SP 800-218r2/SSDF)
- Hardware Security (Program Development)

Develop: *International Standards*
- C-SCRM Specific: e.g., ISO/IEC, Open Group
- Industry Specific: e.g., Telecom, electronics manufacturing

For more info visit: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

Create: *Interagency Policy*
- Telecom
- Micro Electronics

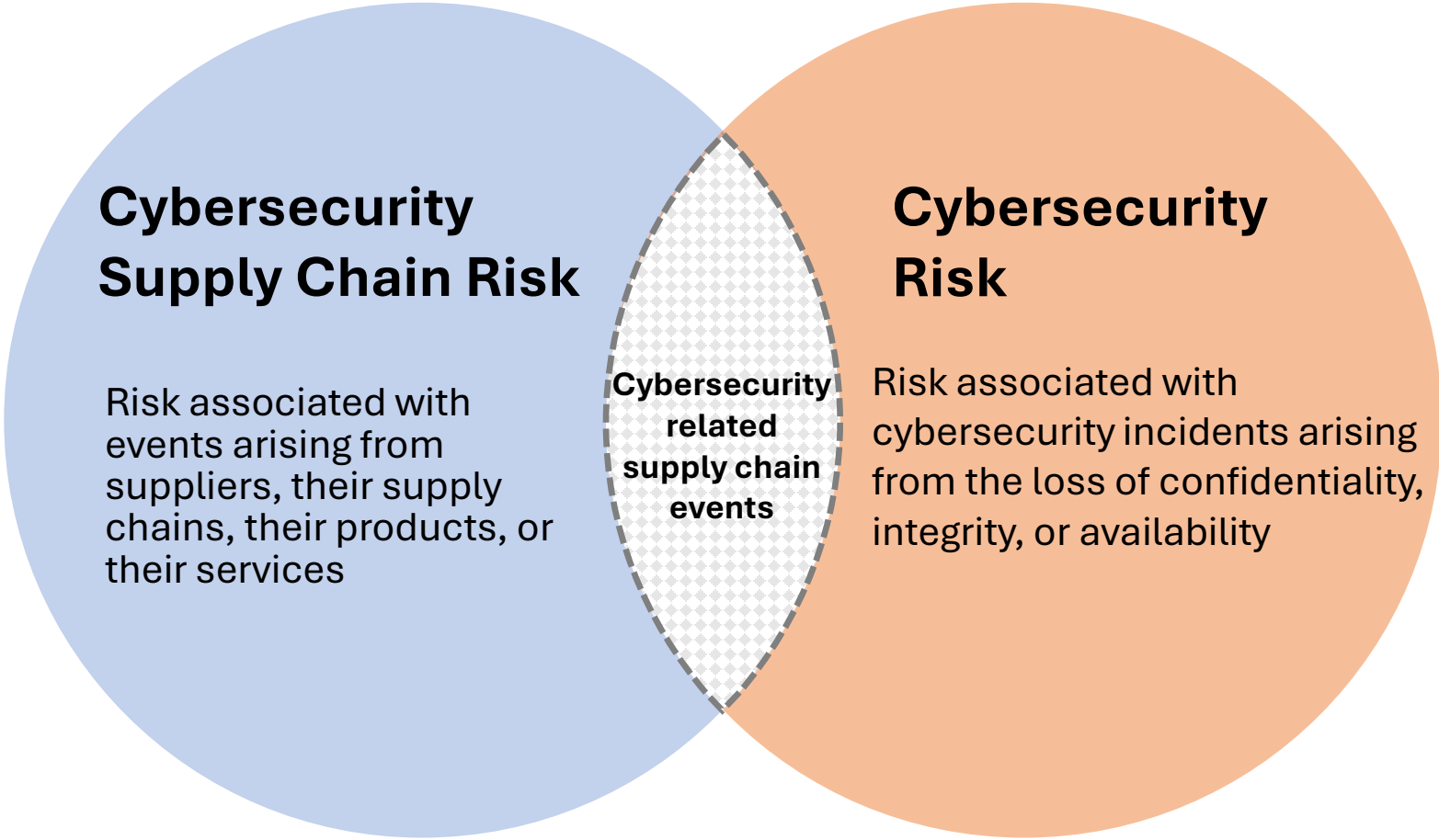
Participate: *As Member of the* Federal Acquisition Security Council (FASC)

Facilitate: *C-SCRM Knowledge Sharing* Software and Supply Chain Assurance Forum (SSCA)

or contact: scrm-nist@nist.gov

C-SCRM involves *identifying, assessing*, and *mitigating* the *risks* associated *with* the *distributed and interconnected nature* of ICT/OT *(information communications technology/operational technology)* *product and service supply chains*. It covers the entire life cycle *(design, development, distribution, deployment, acquisition, maintenance, and destruction)* of a system.

What's the relationship between Cybersecurity Risk and Cybersecurity Supply Chain Risk?




How can cyber threats be introduced into supply chains?

Examples of cyber threat introduction include:

1. Supply chain disruptions
2. Counterfeit or tampered with products
3. System and network vulnerabilities from service partners
4. Malware inserted during repair service
5. Poor quality manufacturing, development, maintenance, or disposal/end of life practices

How can small businesses prepare for cyber supply chain risk?

Prepare for cyber supply chain risk by outlining your:

- Mission and business goals (and associated risks)
- Overall supply chain (and any areas to prioritize mitigating risk for)
- Critical assets
- Resources available for managing risk

Who in an organization should be responsible for C-SCRM?

Concepts to Consider When Planning C-SCRM Responsibilities

- Deciding reasonable goals for C-SCRM work done with limited resources
- Choosing C-SCRM priorities when there are not enough resources for a dedicated C-SCRM role
- Incorporating basic due diligence into day to day business practices
- Planning to scale C-SCRM work along with business

What NIST Resources Are Available for Learning About C-SCRM?

NIST C-SCRM Resources

Finalized Resources

- NIST C-SCRM Computer Security Resource Center (CSRC) Page
- NIST C-SCRM Fact Sheet*
- Special Publication (SP) 800-161 Revision 1 *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- SP 1305 *NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)*

*updated version available soon

Resources in Progress *(finalized versions available soon)*

- SP 800-18 Revision 2 initial public draft (ipd) *Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems*
- SP 1326 (ipd) *NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide*

Special Publication (SP) 800-161 Revision 1: *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*

Additional Information

Moving C-SCRM Practices Toward Maturity

General Wayfinding Tips:

To check which sections of 161 may be applicable to your organization (split by work role), start with the **Audience Profiles and Document Use Guidance** (section 1.4; page 5).

Another option for getting started with 800-161 is the **C-SCRM Key Practices Section** (section 3.4; page 46)

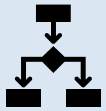
- Foundational Practices
- Sustaining Practices
- Enhancing Practices

800-161r1 Appendix Summary

Appendix A: *C-SCRM Security Controls* (p. 63)

Appendix B: *C-SCRM Control Summary* (p. 164)

Appendix C: *Risk Exposure Framework* (p. 172)



Appendix D: *C-SCRM Templates (p. 196)*

Appendix E: *FASCSA Guidance (p. 230)*

Appendix F: *Response to E.O. 14028 Controls* (p. 247)

Appendix G: *C-SCRM Activities in the Risk Management Process* (p. 248)

Appendix H: *Glossary* (p. 292)

Appendix I: *Acronyms (p. 299)*

Appendix J: *Resources (p. 306)*

800-161r1 Appendix E

 BASELINE RISK FACTORS/RISK INDICATORS	 ASSESSMENT "RECORD" DOCUMENTATION	 USE OF THE SUPPLY CHAIN RISK SEVERITY SCHEMA
Inclusive of adversarial and non-adversarial concerns Grouped into 2 broad categories: • Acquirer-side (Gov't) • & Supply-side Mandatory factors when assessing risk for all things "critical" Agencies should augment/tailor factors to their specific use case.	Guidance communicates expectations about what information needs to be included in an assessment "record" Establishes *[or, begins to establish]* a robust and defensible record Promotes consistency in the scope and organization of documented content to facilitate comparability, re-usability, and information sharing.	Reference to help determine appropriate risk response Mirrors intent/structure of Cyber Incident Severity Schema Helps ensure a common view of: • severity of assessed risk; • urgency required for risk response; • seniority level necessary for coordinating/risk response decision • Info, documentation, and processes to inform/support risk response.

800-161r1: Related Publications and Resources

NIST Special Publication (SP) 800-37

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

NIST Special Publication (SP) 800-39

Managing Information Security Risk: Organization, Mission, and System Information View

NIST Special Publication (SP) 800-53

Security and Privacy Controls for Information Systems and Organizations

NIST Cybersecurity Framework (CSF) 2.0

NIST CWSP 29

NIST Internal Report (NISTIR) 8179

Criticality Analysis Process Model: Prioritizing Systems and Components

NIST Internal Report (NISTIR) 8276

Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

Resource Explanation: Part 1

Special Publication (SP) 800-37: process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. 7 steps: prepare, categorize, select (SP 800-53), implement, assess, authorize, monitor.

Special Publication (SP) 800-39: Organizational Risk Management Strategy (highlight how an organization intends to assess, respond to, and monitor risk)

Special Publication (SP) 800-53: Comprehensive and flexible catalog of security and privacy controls that meet current and anticipated future needs based on changing threats, vulnerabilities, requirements, and technologies. Also provides a common language for discussing security, privacy, and risk management concepts, which improves organizational communication.

See also: NIST Intro Courses for 800-53 (53, 53A, and 53B), as well as crosswalks to other publications (Cybersecurity Framework, Privacy Framework, ISO 27001) and standards (e.g., FIPS 200 (minimum control requirements for each control family))

Resource Explanation: Part 2

Cybersecurity Framework (CSF) 2.0: How to manage cyber risk for federal gov't, industry, and other orgs (and communicate about cyber efforts). High level outcomes applicable to any org (regardless of sector, size, maturity). See also Cybersecurity Framework (CSF) Quick Start Guides (QSGs) [e.g., NIST Special Publication (SP) 1303 (CSF 2.0 + Enterprise Risk Management)].

NIST Internal Report (NISTIR) 8179: Helps organizations identify those systems and components that are most vital and which may need additional security or other protections (also relevant to third party products and services). **Note:** this is control RA-9 (for Criticality Analysis) in 800-53r5 (see pg. 247).

NIST Internal Report (NISTIR) 8276: Key Practices that an organization (of any size, scope, or complexity) can use to manage cybersecurity risks associated with their supply chains. 24 actionable recommendations.

Cybersecurity and Privacy Reference Tool (CPRT): Provides a centralized, standardized, and modernized mechanism for managing reference datasets (and offers a consistent format for accessing reference data from various NIST cybersecurity and privacy standards, guidelines and Frameworks). File formats for Excel and JSON.

What Other Resources Might be Helpful for Learning About C-SCRM?

You May Be Able to Receive Additional C-SCRM Support From

- Federal C-SCRM programming open to the public
- Trade Associations
- Working group(s) specific to your industry
- Local universities (e.g., C-SCRM seminars/learning opportunities, related conferences/forums)
- Supply chain professional development groups (if C-SCRM programming is offered)

CONTACT NIST

About C-SCRM

Website:
https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

Email:
scrm-nist@nist.gov

Google Group:
sw.assurance@list.nist.gov

Forum:
https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca

Glossary

Important Terms

- **Supply chain**: linked set of resources and processes between and among multiple levels of an enterprise

- **Cybersecurity risks throughout the supply chain**: potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services.

Risks *are a result of:*

- **threats** *that* **exploit vulnerabilities within** *the* **products or services** *moving through the supply chain*
- **threats that exploit vulnerabilities** *or exposures* **within the supply chain itself**.

Important Terms Continued

- **Provenance***- timeline of the origin, development, ownership, location, and changes to a system or system component and associated data.

*Provenance may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.

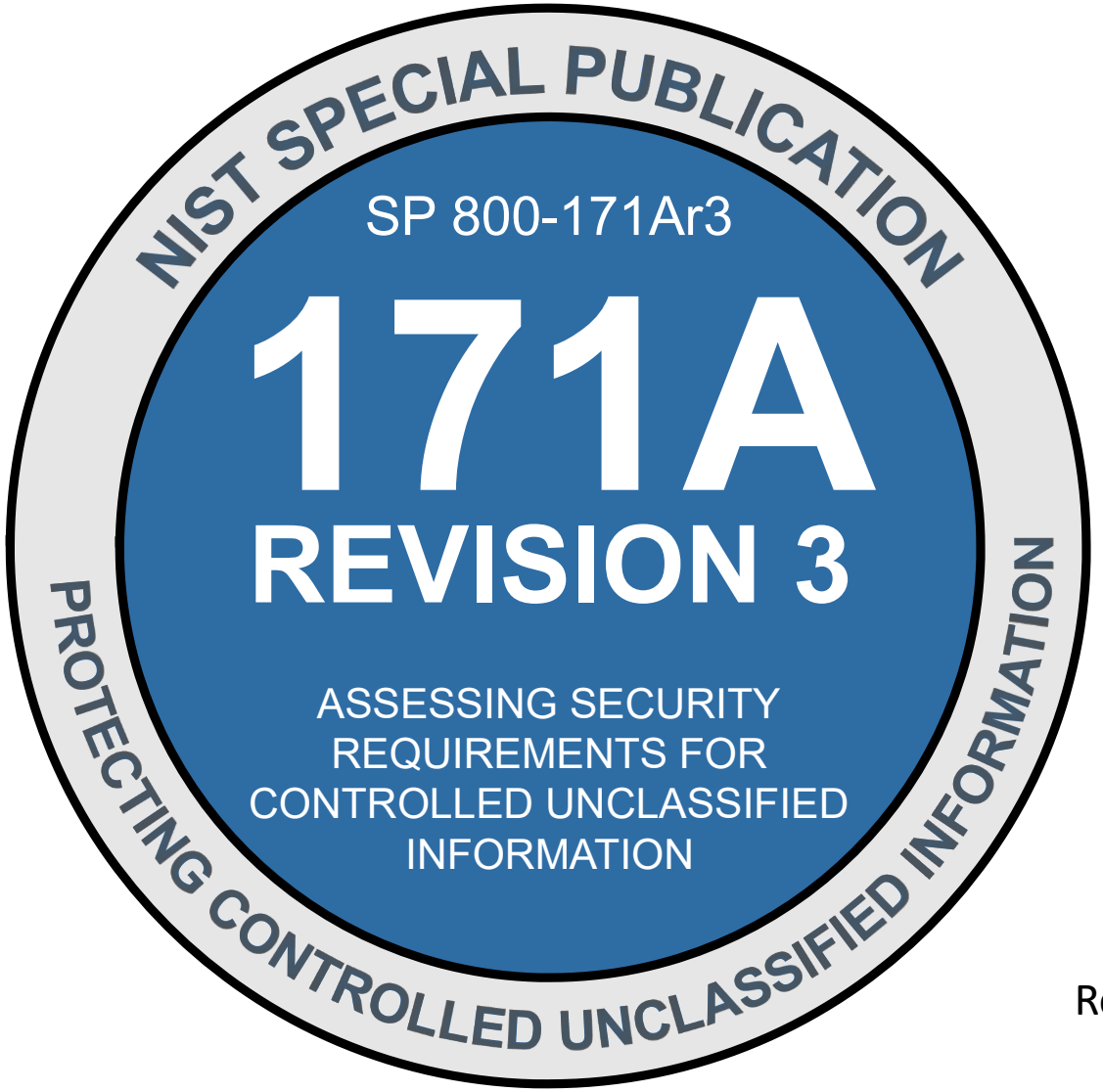
- **Pedigree****- validation of the composition and provenance of technologies, products, and services

**Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid.

Provenance and pedigree are key to doing basic due diligence before acquiring a system, product or service. For more information on due diligence see Special Publication (SP) 1326, a Due Diligence Assessment Quick Start Guide.

Credit: Shutterstock

What's Next?



As we develop a small business resource for SP 800-171A, we'd like your input:

- Are there specific areas or topics within SP 800-171A you'd like to see us focus attention on?
- What questions do you have for SP 800-171A that you'd like to see answered in an SMB resource?

Add responses in chat or you can also email thoughts to: smallbizsecurity@nist.gov

Related Resource: NIST SP 800-171, R3 Small Business Primer: https://doi.org/10.6028/NIST.SP.1318

Next Call

September 16, 2026
2:00p.m. – 3:00p.m. ET

Topic: TBD

nist.gov/itl/smallbusinesscyber/join-community-interest

Discussion and Wrap-Up

https://www.nist.gov/itl/smallbusinesscyber

Daniel.eliot@nist.gov

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE