

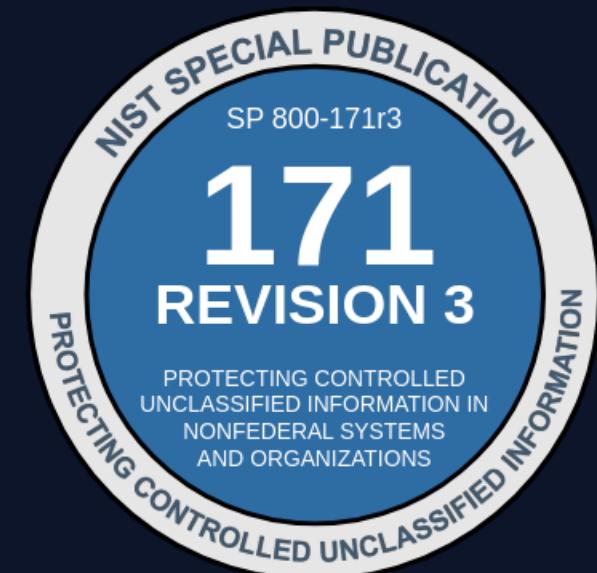
NIST Small Business Cybersecurity Webinar

Protecting Controlled Unclassified Information:
Overview of the NIST Special Publication 800-171, R3

Small Business Primer

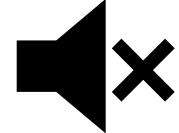


January 20, 2026
1:00 PM – 2:00 PM EST



This webinar is being recorded

Notes and Reminders



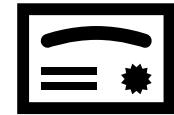
Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.



Webinar recording: This webinar will be recorded and posted here: nist.gov/itl/smallbusinesscyber/events Registrants will be notified via email when the recording is available.



Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



CEU/CPE credits: NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

Agenda



- Brief overview of the NIST Small Business Cybersecurity (SMB) Program
- Introduction to the SP 800-171r3 SMB Primer
 - Development
 - Overview of CUI and SP 800-171r3
 - Key differences between SP 800-171 Revision 2 and Revision 3
 - Getting Started
- What's Next?
- FAQs and Q&A



**Cybersecurity Enhancement
Act of 2014**
Public Law No: 113-274

**NIST Small Business
Cybersecurity Act**
Public Law No: 115-236

Disseminate cybersecurity technical standards and best practices that small business may use voluntarily to help identify, assess, manage, and reduce their cybersecurity risks.

NIST SMB Cybersecurity Resources



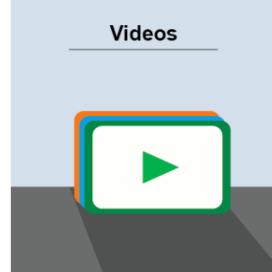
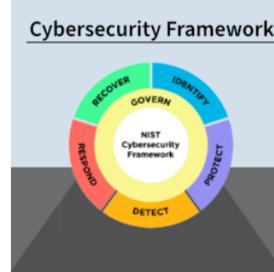
SMALL BUSINESS CYBERSECURITY CORNER

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



NIST Cybersecurity White Paper
NIST CSWP 28

Security Segmentation in a Small Manufacturing Environment

Dr. Michael Powell
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

John Hoyt
Aslam Sherule
Dr. Lynette Wilcox
The MITRE Corporation

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.28>

April 6, 2023

Building Your Small Business' Cybersecurity Team: From In-House to Outsourcing



As small businesses have become more reliant upon data and technology to operate and scale a modern business,

business risks (e.g., financial risks, ant vigilance and continuous ; you might not be a cybersecurity risks and integrating good security-ready team. The k level, cybersecurity or privacy w staff or upskilling existing), to an if all the above.

get started and finding the ions, ideas, and resources for small vides ideas and resources for



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

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1300-2
<https://doi.org/10.6028/NIST.SP.1300-2>
February 2023

www.nist.gov/itl/smallbusinesscyber



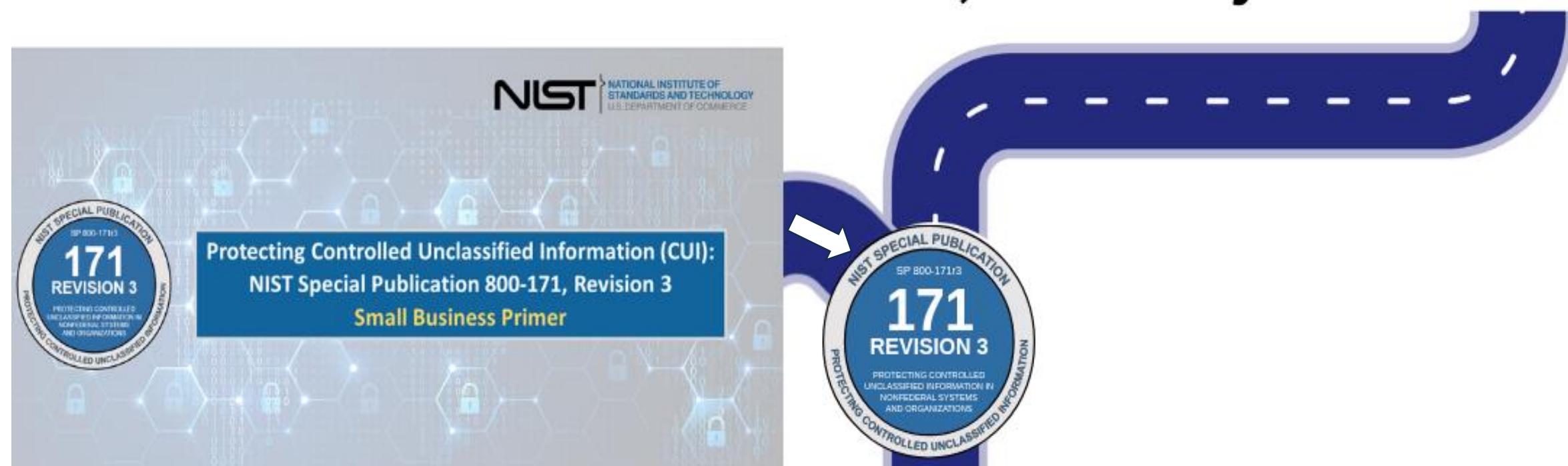
Convening companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work and assist NIST to better meet the cybersecurity needs of small businesses.

Over 20,000
individuals have
already joined the full
COI since
March 6, 2023.

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

2026 meetings:
• February 18
• June 10
• September 16

SP 1318 Small Business Primer as an On-Ramp to the SP 800-171, R3 Journey



<https://doi.org/10.6028/NIST.SP.1318>

Content for Two Audiences

Overview



Purpose of this Primer

This guide provides small businesses with an overview of NIST Special Publication (SP) 800-171 Revision 3, [Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#). The following pages contain:

- An overview of foundational components of SP 800-171
- A list of frequently asked questions and their answers
- Tips for getting started
- Related resources

What is Controlled Unclassified Information (CUI)?*

CUI is information the government creates or possesses, or that an entity creates or possesses on behalf of the government, that law, regulation, or governmentwide policy requires you to take technical and operational steps to protect. Systems that process, store, and transmit CUI often support government programs involving sensitive critical assets. As part of a contractual agreement with the federal government, or possibly with other organizations like municipal governments, prime contractors, universities, etc., you will likely be required to demonstrate you are taking adequate measures to protect CUI. [Examples of CUI](#) include:

	When provided as part of a government contract, examples include:	Marking ¹
Controlled Technical Information	e.g., research and engineering data, engineering drawings, specifications, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.	CUI//SP-CTI
General Proprietary Business Information	e.g., financial information, trade secrets, product research and development, existing and future product designs and performance specifications.	CUI//PROPIN

Even if you do not handle CUI, implementing the security requirements in SP 800-171 will help you take appropriate measures to protect the confidentiality of sensitive information.

Audience
Pages 2-6 provide a **general overview** of SP 800-171, R3—helpful to business leaders or those new to SP 800-171.

Pages 7-27 are for those who are tasked with **managing the implementation** SP 800-171. It is not all-encompassing, but it does provide tips and resources to help with getting started. This section serves as a bridge to the larger SP 800-171 publication.

Key Term: Confidentiality
Confidentiality refers to the protection of information from **unauthorized access and disclosure**.

*Definitions in this document are intended as plain language. View the official definition within [32 CFR Part 2002 "Controlled Unclassified Information."](#)

Introductory Tips for Implementers



What to Expect

The following pages delve deeper into the SP 800-171 R3 publication to provide more details for those responsible for implementing the requirements³. The following pages cover:



Page 8: Key differences between SP 800-171 R2 and R3.

Pages 9-10: General tips for getting started.

Pages 11-28: Tips for getting started, broken out by Control Family.

³ We provide links to non-NIST sites throughout this publication because they may have information of interest to readers. NIST does not necessarily endorse the views expressed or the facts presented on those sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.



Pages 2-6 provide a **general overview** of SP 800-171, R3—helpful to business leaders or those new to SP 800-171.



Pages 7-27 are for those who are tasked with **managing the implementation** SP 800-171.

¹ For more information on types of CUI and markings, visit the National Archives and Records Administration (NARA) <https://www.archives.gov/cui>.

What is CUI?

Controlled Unclassified Information (CUI)

Information requiring protection as identified in a law, regulation, or government-wide policy.

The CUI Registry provides information on the specific categories and subcategories of information that the Executive branch protects.

The CUI Registry can be found at: <https://www.archives.gov/cui>



CUI includes, but is not limited to:

- Privacy (including Health)
- Tax
- Law Enforcement
- Critical Infrastructure
- Controlled Technical Information
- Financial
- Intelligence
- Privilege
- Unclassified Nuclear
- Procurement and Acquisition

CUI Security Requirements Users



Serves as the CUI Executive Agent;
Information Security Oversight
Office (ISOO) performs duties



Developed CUI security
requirements based
on FIPS 200 and SP 800-53
moderate control
baseline tailored to address
confidentiality



Federal Acquisition Regulation (FAR)



All federal contracts where CUI is
stored, transmitted, or processed by
a non-federal organization



**Defense Federal Acquisition Regulation Supplement (DFARS)
and DoD Cybersecurity Maturity Model Certification**



Defense Industrial Base where CUI is
stored, transmitted, or processed by a
non-federal organization

Protecting CUI Series...at a Glance



SECURITY REQUIREMENTS

FOR PROTECTING THE CONFIDENTIALITY OF CUI



NONFEDERAL SYSTEMS & ORGANIZATIONS



PROCESSING, STORING, OR TRANSMITTING CUI



TAILORED FROM THE SP 800-53B

MODERATE BASELINE



INTERNATIONAL USE & IMPACT



NEW & IMPROVED SUPPLEMENTAL RESOURCES



ASSESSMENT PROCEDURES

SP 800-171A



ENHANCED SECURITY REQUIREMENTS

SP 800-172



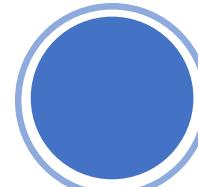
ASSESSMENT PROCEDURES FOR ENHANCED SECURITY REQUIREMENTS

SP 800-172A

What's New: SP 800-171, Rev 3

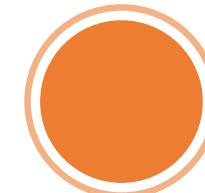
Improved Readability

- Streamlined “Introduction” and “The Fundamentals” sections

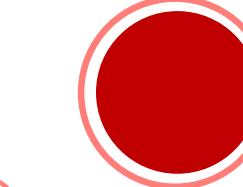


Updated Security Requirements

- Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in SP 800-53B
- Eliminated distinction between basic & derived requirements
- Increased specificity & grouped requirements
- Introduced organization-defined parameters (ODPs)
- Removed outdated & redundant requirements
- Further tailored discussions to focus on CUI



Significant Changes



Updated Tailoring Criteria

- Added new tailoring categories, NA and ORC
- Eliminated NFO tailoring category
- Recategorized selected controls from SP 800-53B moderate baseline



Added Supplemental Resources

- CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
- Developed Updated FAQ
- Concurrently issued updated security requirements through Cybersecurity and Privacy Reference Tool

SP 800-171 Rev 2 withdrawn: May 14, 2024

Getting Started with SP 800-171, R3



- Determine if your business has CUI.
- Understand how CUI flows into, within, and out of the business.
- Identify the role(s) responsible for security and provide the necessary resources.
- It's not all technology.
- Implement the requirements and document implementation in a system security plan.
- Create a plan of action and milestones (POAM).
- Find help when you need it.
- Review SP 800-171A Rev. 3.



COMING
IN

What's Next?



As we begin to 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?
- Is there a particular format you'd prefer the resource be in (video, fact sheet, primer, etc.)?

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

Upcoming Webinar

Resources for Ransomware Risk Management

 January 28, 2026
2:00 PM-3:00 PM EST



<https://www.nist.gov/itl/smallbusinesscyber/events>



How can I “comply” with SP 800-171?

How do I know if I have CUI?

How do I get a “NIST SP 800-171 Assessment”?

What products, vendors, or solutions are “NIST SP 800-171 compliant” or “CMMC-certified”?

What is the relationship between NIST and CMMC?

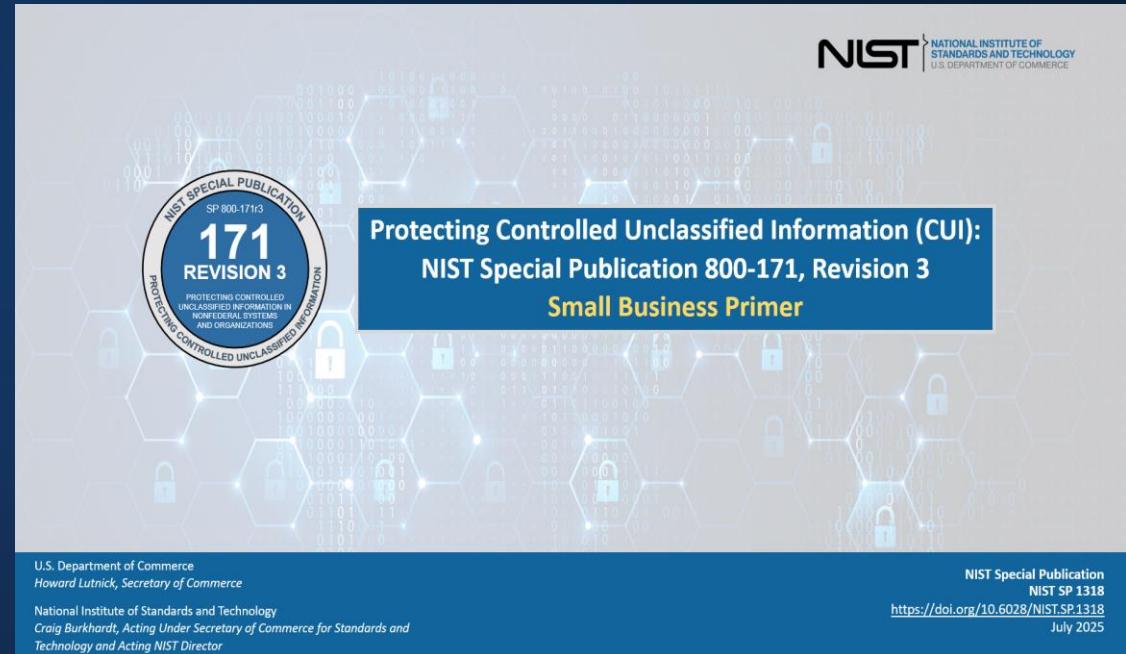
Page 5 of the Primer.

View more FAQs [here](#).

Q & A

Questions for Attendees:

- Are there additional webinar topics you'd like to see us cover regarding the NIST CUI series?
- Is there another publication or topic you would like to see a NIST small business resource created for?
- What types of resources would you like to see more of?



Links

- **NIST SP 800-171r3 Small Business Primer:** <https://doi.org/10.6028/NIST.SP.1318>
- **Protecting CUI Project Page:** <https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information>
- **Small Business Cybersecurity Corner:** <https://www.nist.gov/itl/smallbusinesscyber>
- **Signing up for NIST email bulletins:** <https://public.govdelivery.com/accounts/USNIST/subscriber/new>
- **NIST Cybersecurity and Privacy Reference Tool:** <https://csrc.nist.gov/projects/cprt/catalog>