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

NIST Small Business Cybersecurity Webinar

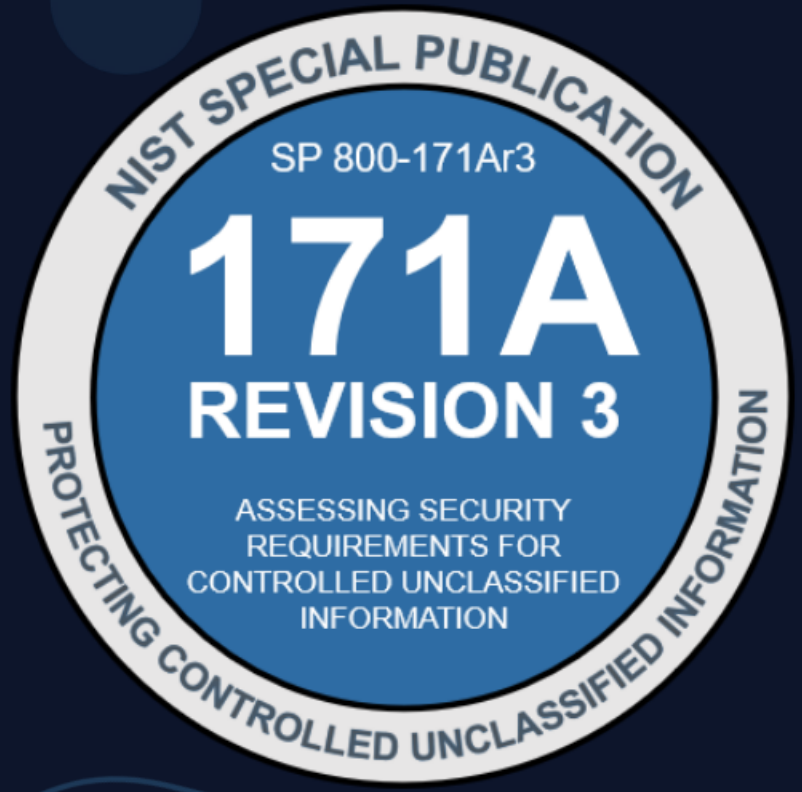
Assessing Security Requirements for Controlled Unclassified Information (CUI): NIST Special Publication 800-171A, Revision 3

Small Business Primer



October 29, 2026

2:00 PM -3:00 PM ET



This webinar is being recorded

Notes and Reminders

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

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



Credit: Shutterstock

- Brief overview of the NIST Small Business Cybersecurity (SMB) Program
- Overview of SP 800-171Ar3 and NIST's Suite of Protecting CUI Resources
- Introduction to the SP 800-171Ar3 SMB Primer
- Additional Resources
- What's Next?
- FAQs and Q&A

Credit: Shutterstock


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

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





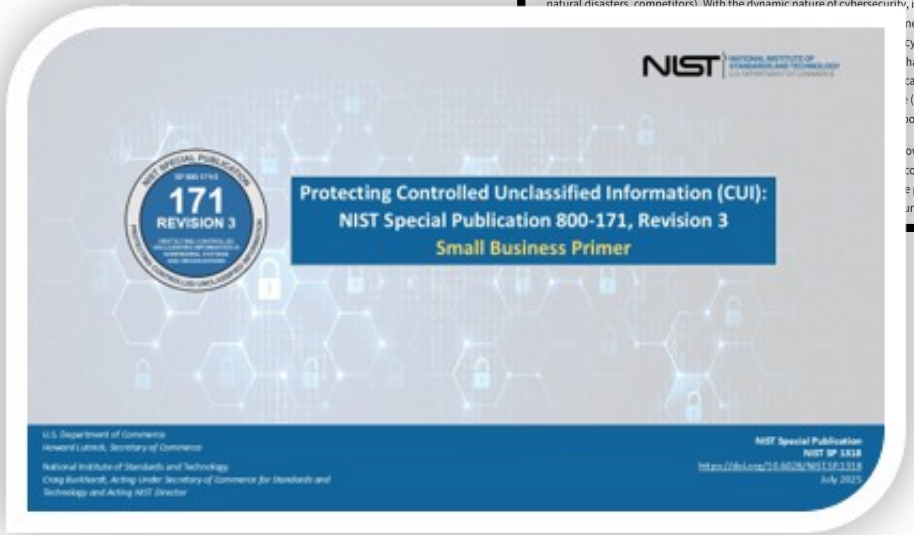
SPOTLIGHT







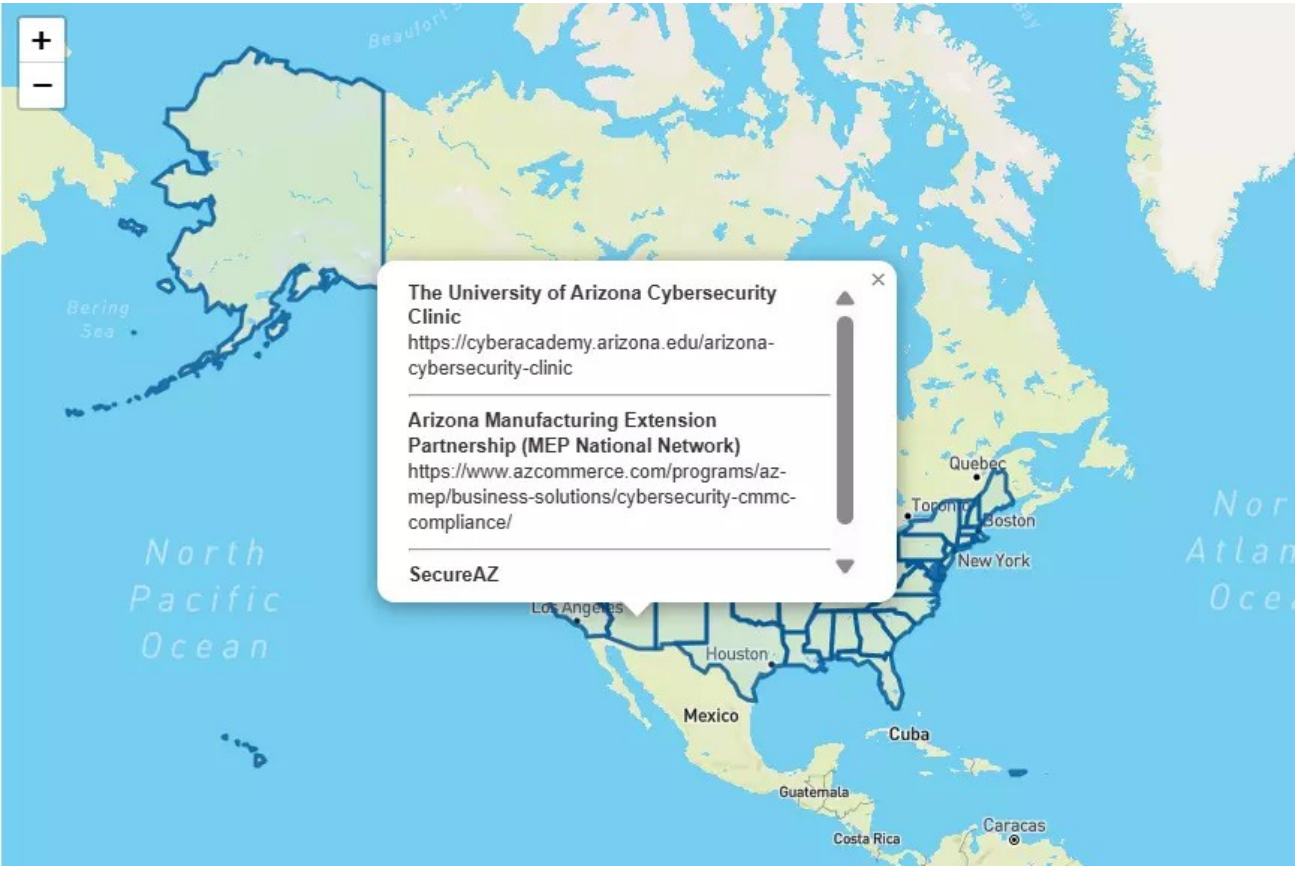




www.nist.gov/itl/smallbusinesscyber

Small Business Cybersecurity Support Programs Finder

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



Search:

State	Program Name	Program URL
AK	Alaska Small Business Development Center	https://aksbdc.org/2026/04/technology-ai-cybersecurity-in-alaska/
AL	University of Alabama Cybersecurity Clinic	https://ida.culverhouse.ua.edu/initiatives/cyber/
AR	Arkansas Economic Development Commission Manufacturing Solutions (MEP National Network)	https://www.mfgsolutions.org/services/cybersecurity/
AZ	The University of Arizona Cybersecurity Clinic	https://cyberacademy.arizona.edu/arizona-cybersecurity-clinic
AZ	Arizona Manufacturing Extension Partnership (MEP National Network)	https://www.azcommerce.com/programs/az-mep/business-solutions/cybersecurity-cmmc-compliance/
AZ	SecureZA	https://secureaz.org/
CA	San Diego Cyber Clinic	https://sdccoe.org/cyber-clinic/

www.nist.gov/itl/smallbusinesscyber/cybersecurity-support-programs-finder

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****.*

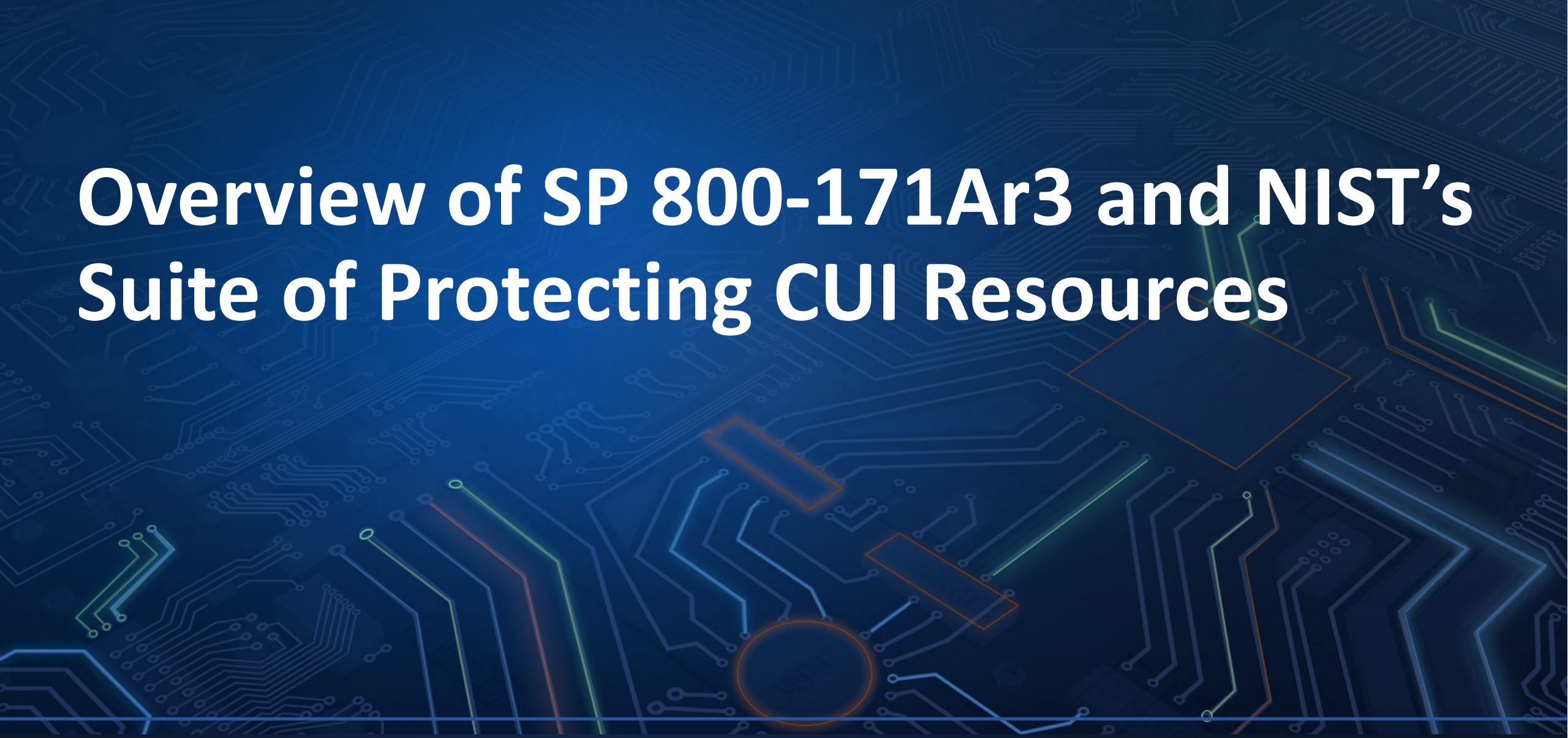
Over 22,000
individuals have already joined the full COI since March 6, 2023.

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

2026 meetings:
- **November 10**
- **February 10**
- **June 10**
- **August 10**

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

Overview of SP 800-171Ar3 and NIST's Suite of Protecting CUI Resources



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

What is CUI?

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

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

NATIONAL ARCHIVES

CONTROLLED UNCLASSIFIED INFORMATION

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 DoW Cybersecurity Maturity Model Certification

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

https://csrc.nist.gov/projects/protecting-CUI

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

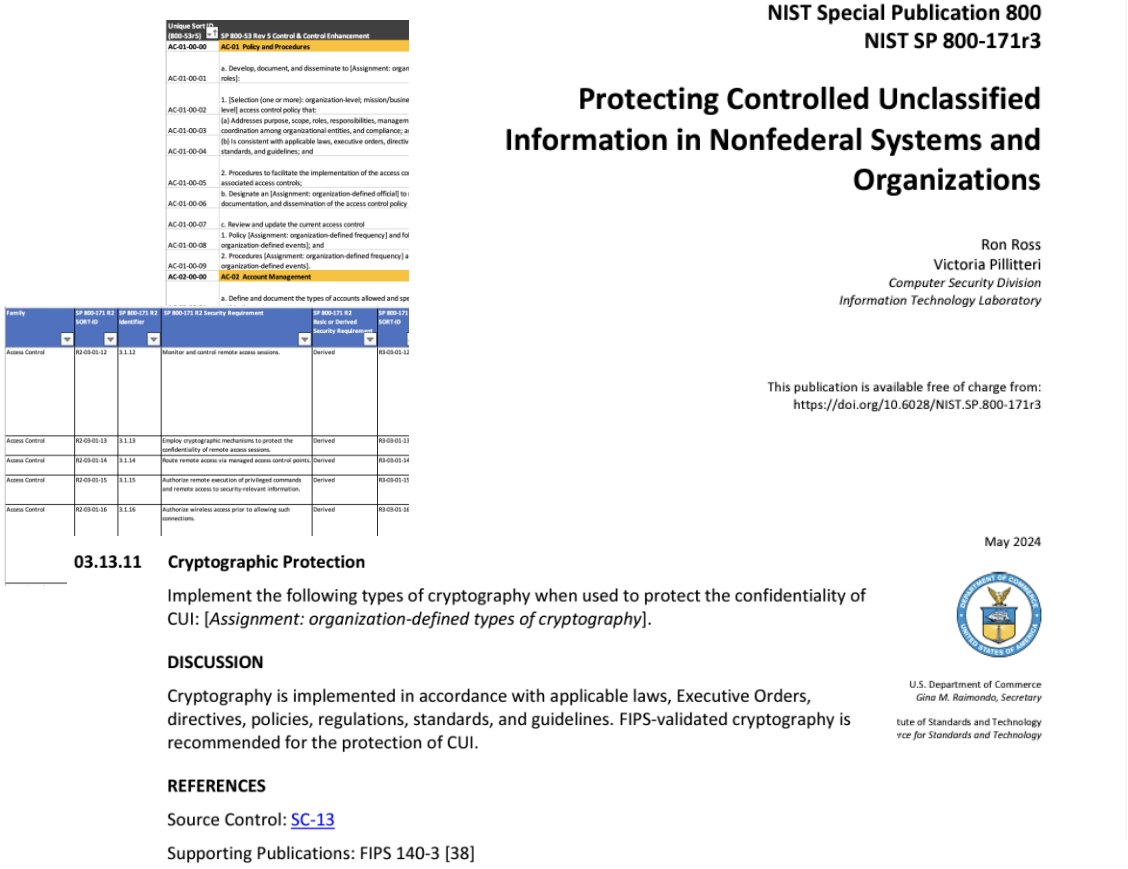
ASSESSMENT PROCEDURES FOR ENHANCED SECURITY REQUIREMENTS
SP 800-172A

Overview: Special Publication (SP) 800-171

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Purpose: Provide federal agencies a set of recommended security requirements for protecting the **confidentiality** of **Controlled Unclassified Information (CUI)** in nonfederal systems and organizations.

Published: Rev. 3 – May 2024
Rev. 2 – Feb 2020; Rev. 1 – Dec 2016
[Updated June 2018]; originally published June 2015



Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement
AC-01-00-00	**AC-01 Policy and Procedures**
AC-01-00-01	a. Develop, document, and disseminate to [Assignment: organ roles]:
AC-01-00-02	1. [Selection (one or more): organization-level; mission/busine level] access control policy that:
AC-01-00-03	(a) Addresses purpose, scope, roles, responsibilities, managem coordination among organizational entities, and compliance; a
AC-01-00-04	(b) Is consistent with applicable laws, executive orders, directiv standards, and guidelines; and
AC-01-00-05	2. Procedures to facilitate the implementation of the access co associated access controls;
AC-01-00-06	b. Designate an [Assignment: organization-defined official] to documentation, and dissemination of the access control policy
AC-01-00-07	c. Review and update the current access control
AC-01-00-08	1. Policy [Assignment: organization-defined frequency] and fo organization-defined events]; and
AC-01-00-09	2. Procedures [Assignment: organization-defined frequency] a organization-defined events].
AC-02-00-00	**AC-02 Account Management**
	a. Define and document the types of accounts allowed and spe

Family	SP 800-171 R2 SORT-ID	SP 800-171 R2 Identifier	SP 800-171 R2 Security Requirement	SP 800-171 R2 Basic or Derived Security Requirement	SP 800-171 SORT-ID
Access Control	R2-03-01-12	3.1.12	Monitor and control remote access sessions.	Derived	R3-03-01-12
Access Control	R2-03-01-13	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Derived	R3-03-01-13
Access Control	R2-03-01-14	3.1.14	Route remote access via managed access control points.	Derived	R3-03-01-14
Access Control	R2-03-01-15	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	Derived	R3-03-01-15
Access Control	R2-03-01-16	3.1.16	Authorize wireless access prior to allowing such connections.	Derived	R3-03-01-16

NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

May 2024

03.13.11 **Cryptographic Protection**

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. FIPS-validated cryptography is recommended for the protection of CUI.

REFERENCES

Source Control: SC-13

Supporting Publications: FIPS 140-3 [38]

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

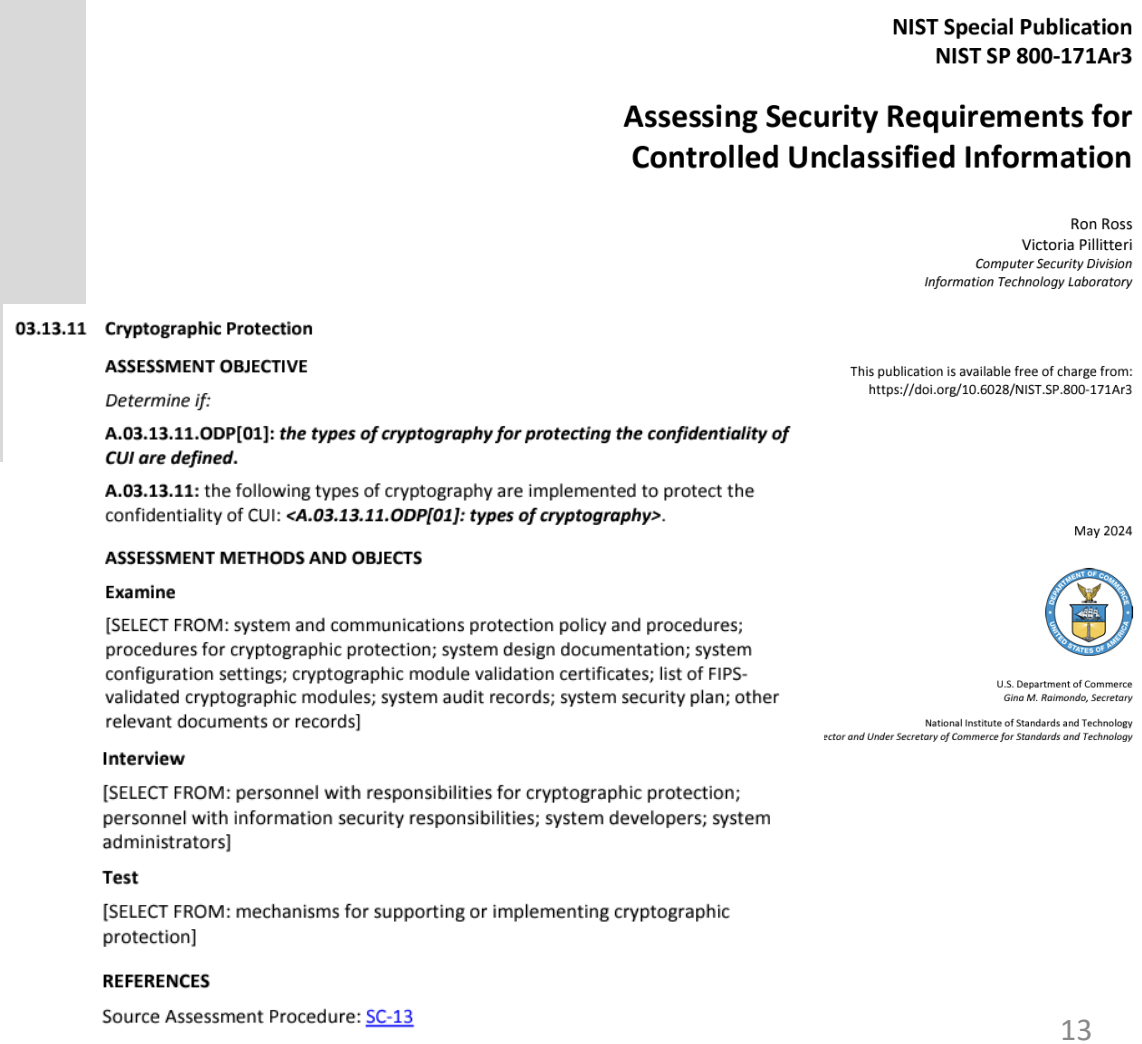
tute of Standards and Technology
rce for Standards and Technology

Overview: SP 800-171A

Assessing Security Requirements for Controlled Unclassified Information

Purpose: Provides **assessment procedures and a methodology** that can be employed to conduct assessments of the **CUI security requirements** in SP 800-171.

Published: Rev. 3 – May 2024*
originally published June 2018



NIST Special Publication
NIST SP 800-171Ar3

Assessing Security Requirements for Controlled Unclassified Information

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

03.13.11 Cryptographic Protection

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.11.ODP[01]: ***the types of cryptography for protecting the confidentiality of CUI are defined.***

A.03.13.11: the following types of cryptography are implemented to protect the confidentiality of CUI: ***<A.03.13.11.ODP[01]: types of cryptography>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for cryptographic protection; system design documentation; system configuration settings; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for cryptographic protection; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting or implementing cryptographic protection]

REFERENCES

Source Assessment Procedure: SC-13

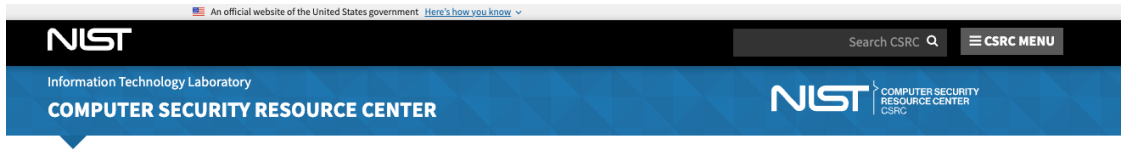
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171Ar3

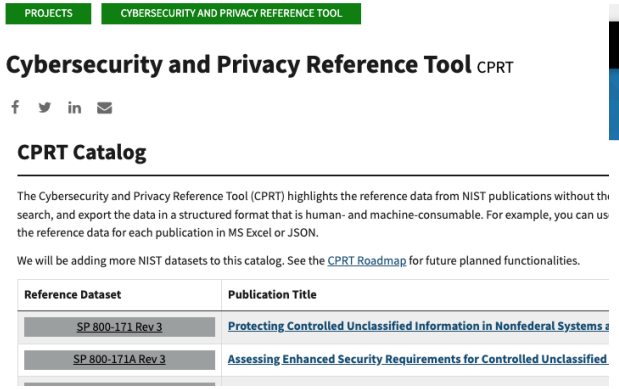
May 2024

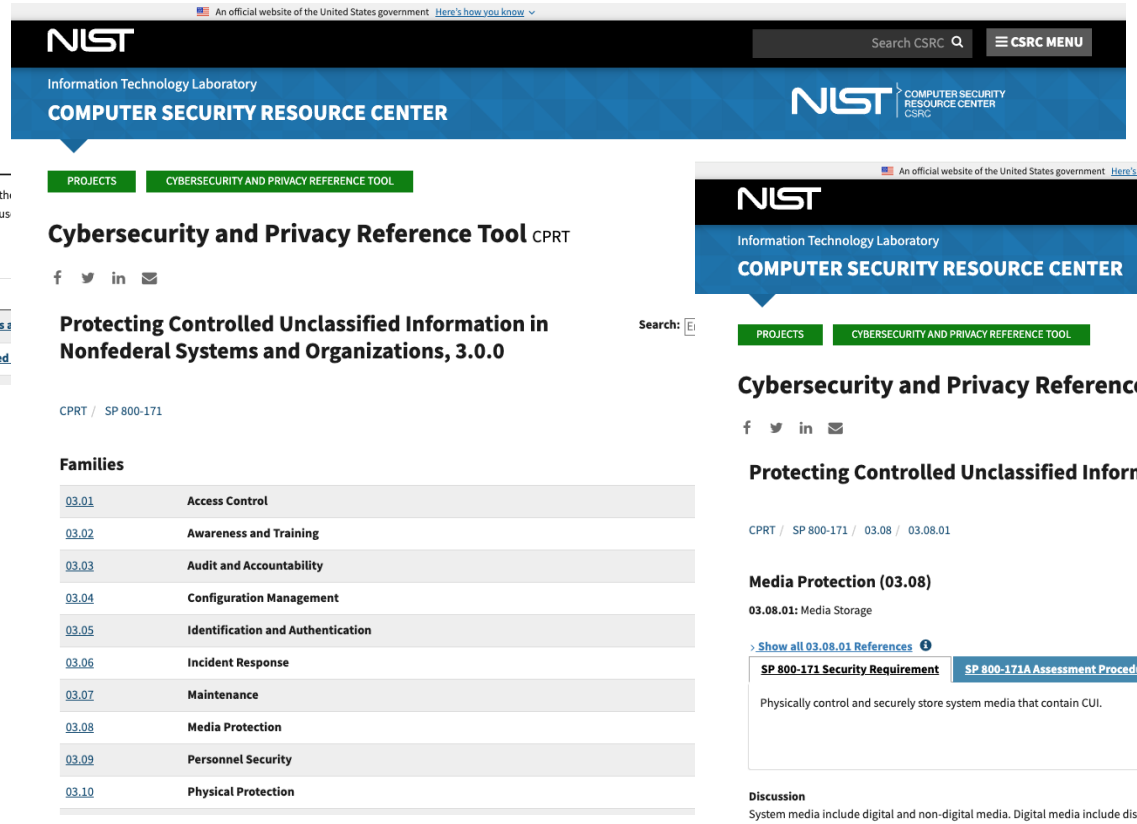
U.S. Department of Commerce
Gina M. Raimondo, Secretary

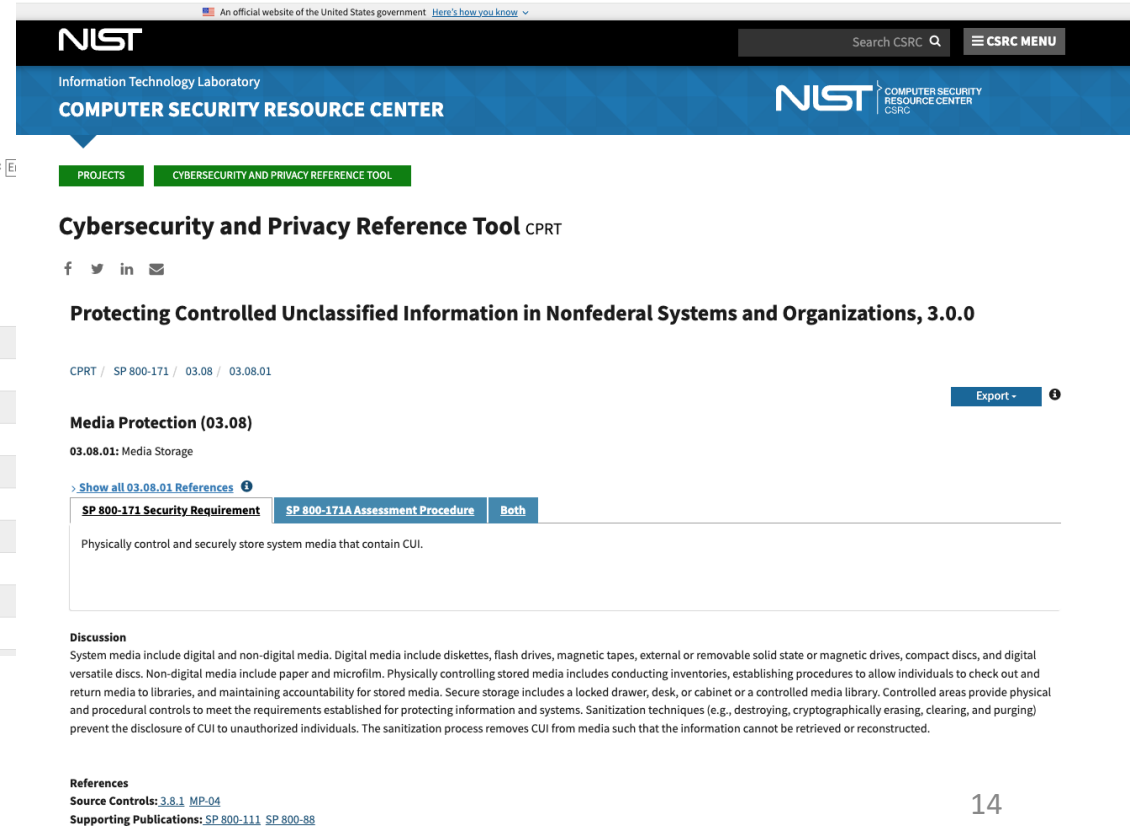
National Institute of Standards and Technology
ector and Under Secretary of Commerce for Standards and Technology

Protecting CUI Guidance as Datasets



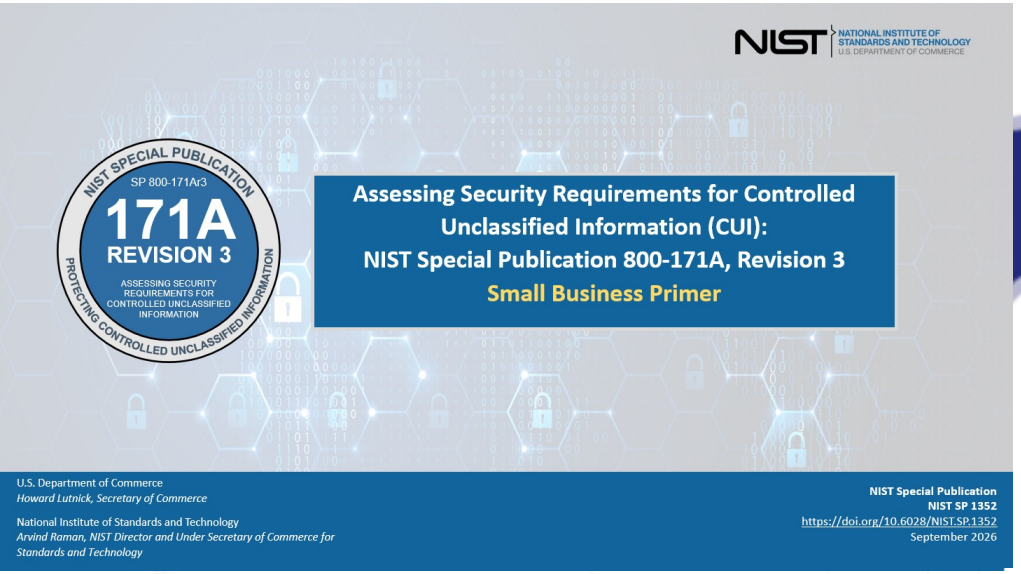






https://csrc.nist.gov/Projects/cprt/catalog#/cprt/home

NIST SP 800-171Ar3 Small Business Primer





https://doi.org/10.6028/NIST.SP.1352

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

What, How, and Who?



Security Requirements
(The What)

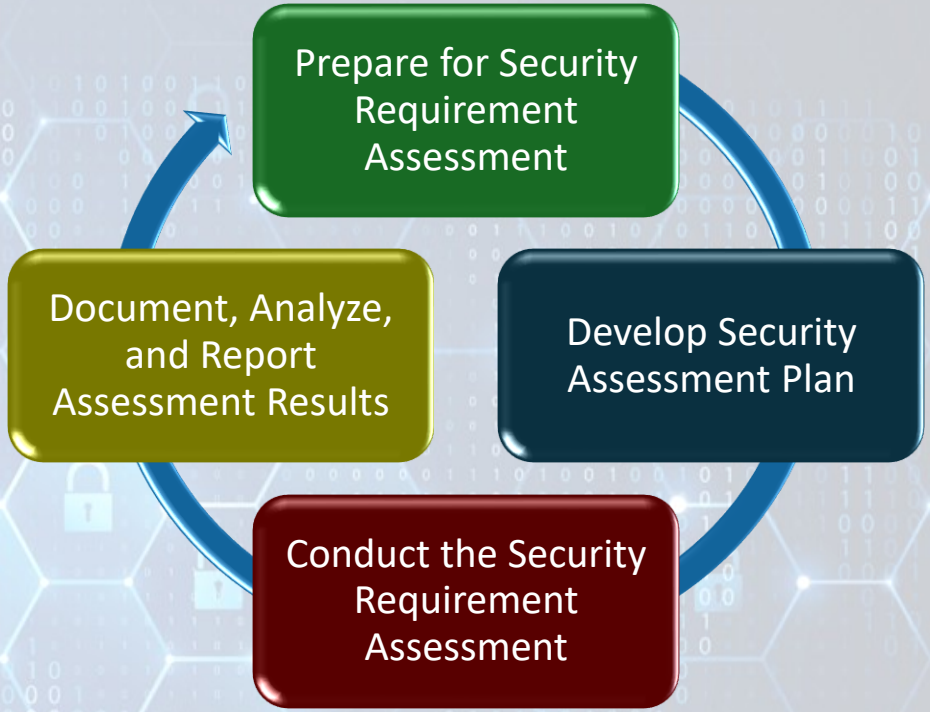
Are We Effectively Implementing the Requirements?
(The How)

Who Conducts Assessments?

The terms “NIST Assessment” and “NIST SP 800-171 Assessment” are frequently used to describe the Department of War (DOW) process used to complete its NIST SP 800-171 Assessment Module through the Supplier Performance Risk System (SPRS).

NIST develops the underlying technical guidelines (SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A) on which the “NIST Assessment” is based, but NIST does not have a role in DOW’s implementation of its programs. Learn more about DOW’s programs here.

Ready, Set, Assess



Business & Assessors prepare; determine scope

Assessors develop assessment plan

Assessor executes assessment plan; provides results & recommendations

Business determines appropriate steps to respond to assessment results

https://csrc.nist.gov/projects/protecting-controlled-unclassified-information

Overview of Assessment Procedures

Assessment Procedure

An assessment procedure consists of an assessment objective and a set of potential assessment methods and objects that can be used to conduct the assessment.

Assessment Objective
(What the assessor is attempting to verify)

A set of evaluation statements that break down the security requirement into smaller, individual parts to see if it is being met.

Potential Assessment Methods
(How an assessor may review)

Example ways to get evidence and artifacts that show that the security requirement is in place, operating as intended, and achieving the desired results. **Not all methods and objects are required.**

Could include

- **Examine**
  Process of reviewing, studying, inspecting, or analyzing assessment objects (such as policies, procedures, System Security Plan, etc.)
- **Interview**
  Process of holding discussions with individuals or groups about assessment objects.
- **Test**
  Process of evaluating implemented controls under specified conditions to compare *actual* with *expected* behavior. Essentially, are controls functioning as they should be?

Potential Assessment Objects
(Evidence the assessor may review)

Identify the specific items being assessed, and can include specifications, mechanisms, activities, and individuals. **Not all methods and objects are required.**

Could include

- **Specifications**
  Documented artifacts[4] (e.g., plans, policies, procedures, requirements, functional and assurance specifications, design documentation, and architectures) associated with a system.
- **Mechanisms**
  Hardware, software, and firmware safeguards implemented within a system.
- **Activities**
  Protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising an incident response plan, and monitoring network traffic).
- **Individuals**
  People applying the specifications, mechanisms, or activities described above.

Note:

Additional methods and objects that demonstrate that the requirement is in place, operating as intended, and achieving the desired result can also be used.

[4] *Artifacts may be in formats other than documents (e.g., databases, Governance, Risk, and Compliance [GRC] tools, or Open Security Controls Assessment Language [OSCAL])*

Sample Security Requirement and Assessment Procedure

SP 800-171r3 Security Requirement Example

03.01.10 Device Lock

a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

SP 800-171Ar3 Assessment Procedure Example

03.01.10 Device Lock

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.10.ODP[01]: one or more of the following PARAMETER VALUES are selected:
{a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}.

A.03.01.10.ODP[02]: the time period of inactivity after which a device lock is initiated is defined (if selected).

A.03.01.10.a: access to the system is prevented by <A.03.01.10.ODP[01]: SELECTED PARAMETER VALUES>.

A.03.01.10.b: the device lock is retained until the user reestablishes access using established identification and authentication procedures.

A.03.01.10.c: information previously visible on the display is concealed via device lock with a publicly viewable image.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for session lock… other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for cryptographic key establishment and/or management; personnel with information security responsibilities; system administrators]

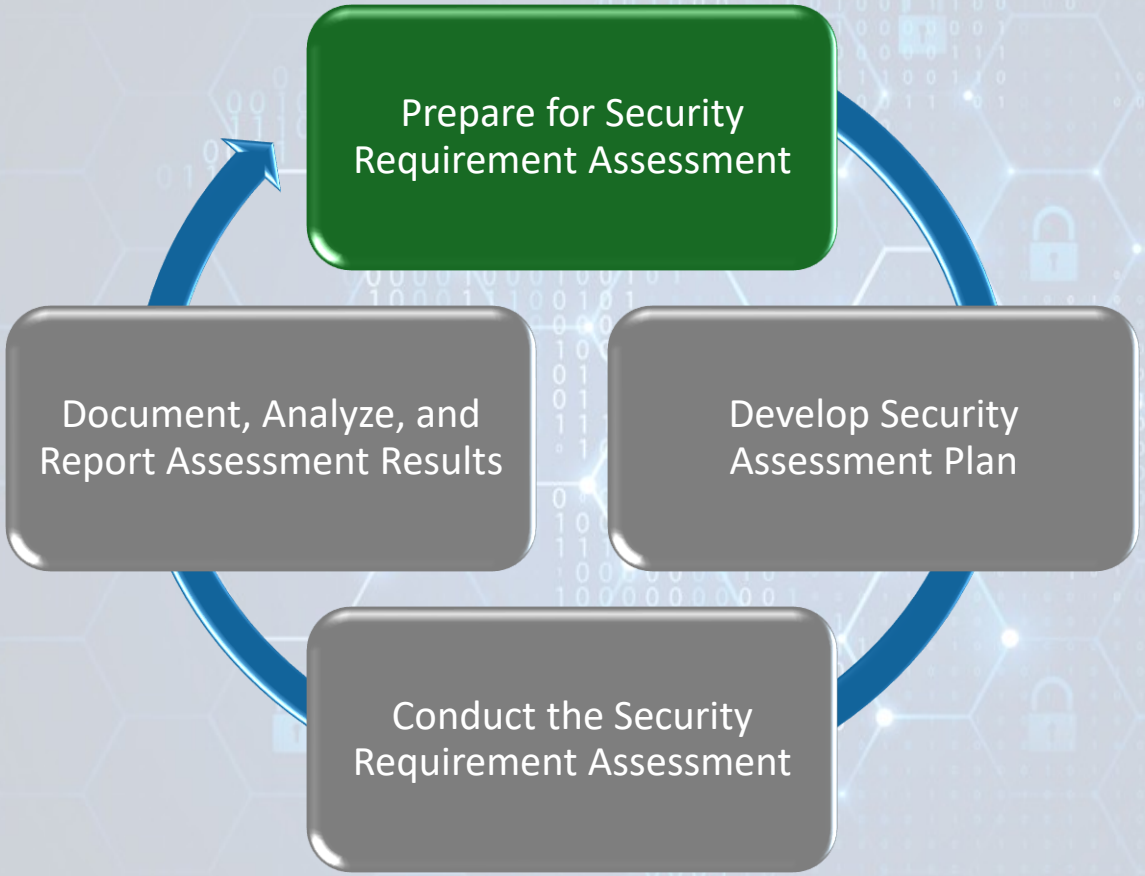
Test

[SELECT FROM: mechanisms for implementing the access control policy for session lock; session lock mechanisms]

REFERENCES

Source Assessment Procedures: AC-11, AC-11(01)

Preparing for the Security Requirement Assessment



Thorough preparation is a critical component to an effective assessment. Preparatory activities address a range of issues relating to the cost, schedule, and performance of the assessment.

Gather other documentation and artifacts, including but not limited to the Plan of Action and Milestones, system security plan, network diagram, policies and procedures, employee manuals, user training records, sample audit logs.

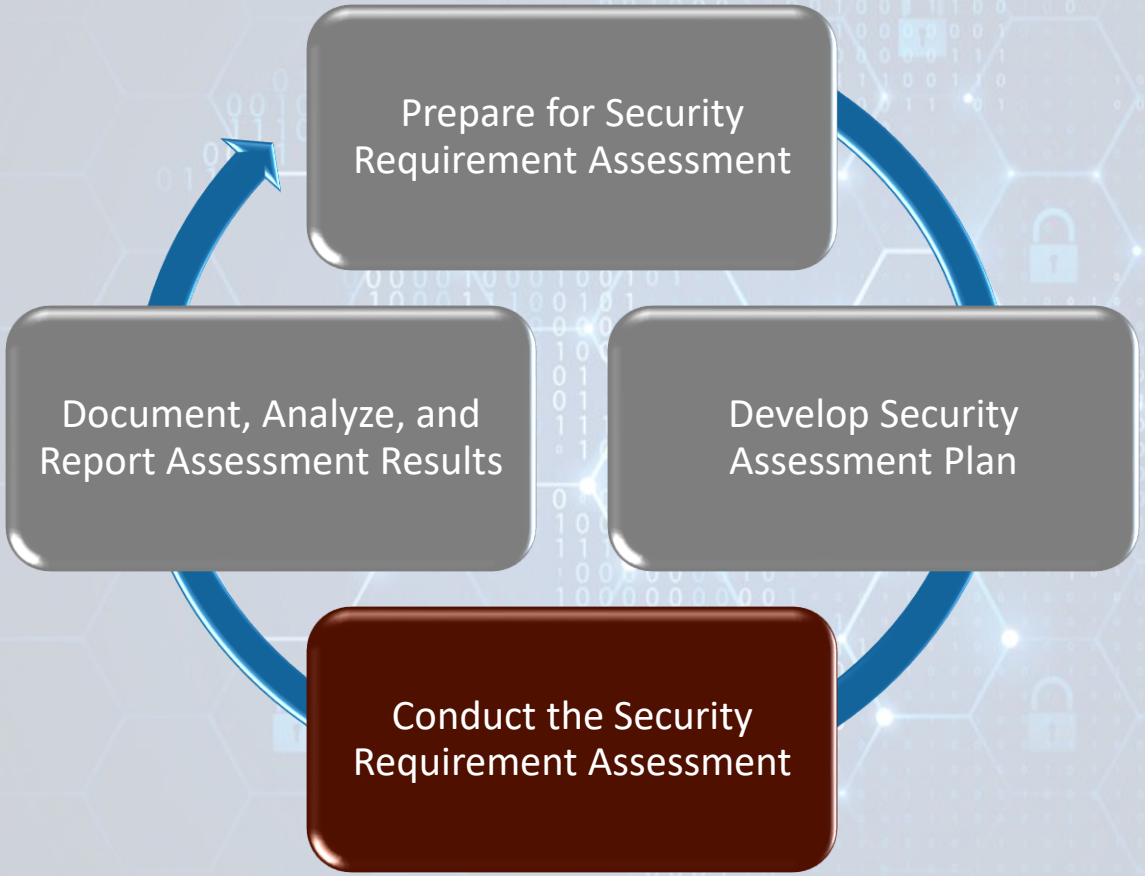
Developing the Security Assessment Plan



The assessment plan establishes the objectives for the security requirement assessment and a detailed roadmap of how to conduct the assessment based on the system security plan.

If using an external assessor, they would be creating the assessment plan for the business. However, **business leaders should review the assessment plan** before the assessment begins to ensure it is scoped appropriately, prevents or minimizes disruption to the business operations, etc.

Conduct the Security Requirement Assessment



The goal of an assessment is to verify if the business is effectively implementing the requirements.

Satisfied – Indicates that the assessment objective for the security requirement, or subset of the requirement, addressed by the determination statement has been met and produced an acceptable result.

Other than satisfied – Indicates that the assessment objective for the requirement has not been met and has produced an unacceptable result.

Documenting, Analyzing, and Reporting Assessment Results



The outcome of the assessment for each [SP 800-171A] assessment objective is "satisfied" or "other than satisfied." Every objective is binary; if any single objective is not met, the entire requirement is Not Met.
The *assessment report* details what was evaluated, how it was verified the outcome of the assessment, and any gaps and potential remediations.

Understand what requirements the business has for documenting and acting upon assessment results.

What Happens After the Assessment?

- Review the assessment report; identify any gaps/deficiencies.
- Generate or update:
  - **Plan of Action and Milestones (POA&M):** Every requirement that is Not Met translates to a POA&M and specifies the deficiency, the planned corrective action, resources needed/assigned, and milestone target completion date(s).
  - **System Security Plan (SSP):** Update SSP to reflect the "as implemented" state.
- Determine Score and Report *(if applicable)*
- Implement POA&M
  - Tips: Prioritize High-Impact Gaps, Collect Evidence, Rescore and Resubmit (if applicable)
- Continuously Monitor: good risk management is not a one-and-done exercise!



Additional Resources

NIST SP 800-171r3 Small Business Primer





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

Recording and Q&A Summary Available



Question	Answer
There were multiple questions about the Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC) Program, including recommendations for vendors and how to get certified.	NIST cannot speak on behalf of the CMMC Program. For more information about the CMMC, including additional resources, see https://dodcio.defense.gov/CMMC/.
There were multiple implementation-specific questions.	NIST does not generally comment on or evaluate the implementation of requirements or "compliance." If there are additional questions about NIST's Protecting Controlled Unclassified Information (CUI) series, email sec-cert@nist.gov.
There were multiple questions about which revision of SP 800-171/SP 800-171A to use.	The CMMC Program currently leverages the requirements and assessment procedures in SP 800-171r2 (Revision 2) and SP 800-171A. Organizations can leverage the NIST-created change analysis (SP 800-171r2 to r3) to determine which revision best meets their current and future needs.
What types of small businesses (in which industries) need to meet SP 800-171 requirements? What is the relevance of SP 800-171 to small businesses?	Currently, the defense industrial base is the largest user community of NIST's Protecting CUI series through the Defense Federal Acquisition Regulation Supplement (DFARS) and CMMC requirements. Even if your organization does not have a contract that requires implementation of the SP 800-171 security requirements, you can still elect to use the requirements to protect the confidentiality of any information, even if it is not CUI. Like all NIST cybersecurity and privacy guidelines, the Protecting CUI series

www.nist.gov/news-events/events/2026/01/nist-small-business-cybersecurity-webinar-protecting-controlled

NIST SP 800-53 Online Introductory Courses

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



Security and Privacy Controls Introductory Course

Based on SP 800-53, Security and Privacy Controls for Information Systems and Organizations, the course introduces the SP 800-53 control catalog and each control family.



Assessing Security and Privacy Controls Introductory Course

Based on SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations, the course covers the methodology for assessing the SP 800-53 controls. The material also explains the structure of the assessment procedures and assessment objectives.



Control Baselines Introductory Course

Based on SP 800-53B, Control Baselines for Information Systems and Organizations, the course provides an overview of security and privacy control baselines and guidance for tailoring them.

https://csrc.nist.gov/Projects/risk-management/rmf-courses



Credit: Shutterstock

What's Next?





As we begin to develop a small business resource for SP 800-172r3, we'd like your input:

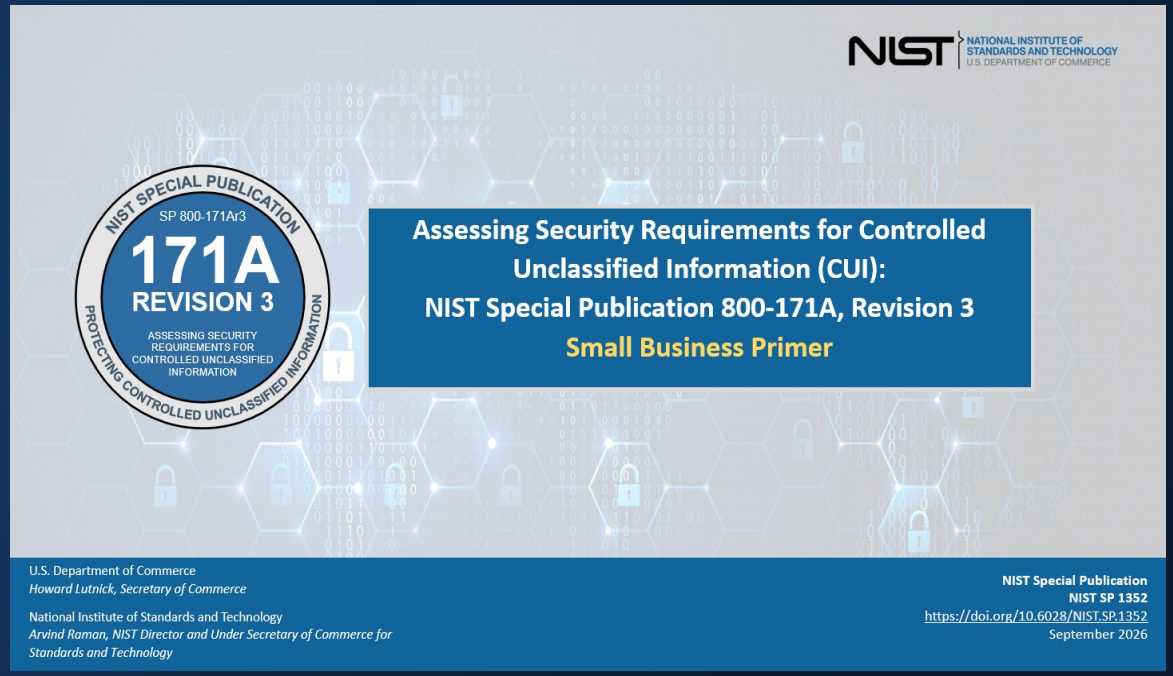
- Are there specific areas or topics within SP 800-172 you'd like to see us focus attention on?
- What questions do you have for SP 800-172 that you'd like to see answered in an SMB resource?
- Is there a particular format you'd prefer the resource be in (video, fact sheet, primer, etc.)?

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

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?



View the recording and Q&A summary from our January 20, 2026, webinar: ***Protecting Controlled Unclassified Information: Overview of the NIST Special Publication 800-171, Revision 3 Small Business Primer*** (https://www.nist.gov/itl/smallbusinesscyber/events)

Links

- **NIST SP 800-171r3 Small Business Primer:** https://doi.org/10.6028/NIST.SP.1352
- **NIST SP 800-171r3 Small Business Primer:** https://doi.org/10.6028/NIST.SP.1318
- **January 20 NIST SP 800-171r3 Small Business Primer Overview Recording and Q&A Summary:** https://www.nist.gov/news-events/events/2026/01/nist-small-business-cybersecurity-webinar-protecting-controlled
- **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