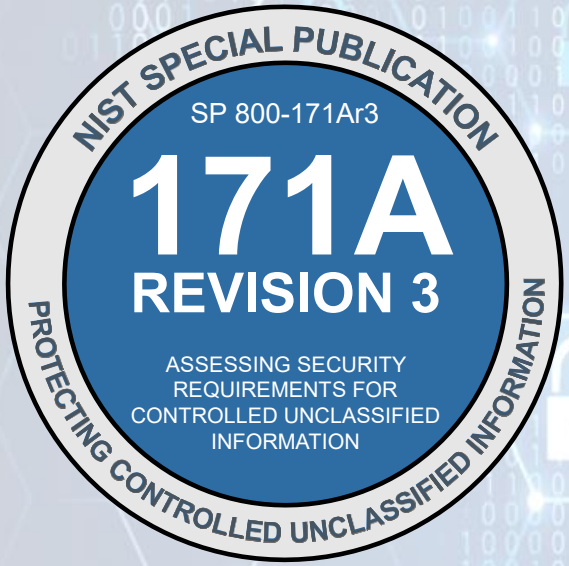
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



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

Small Business Primer

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1352
https://doi.org/10.6028/NIST.SP.1352
September 2026

General Overview

Purpose of this Primer

Small businesses juggle many competing priorities with their limited resources (time, budget, IT staff, etc.). A CUI security assessment can be unfamiliar and intimidating to those new and experienced with CUI security requirements. This guide provides small business owners and operators with a high-level overview of NIST Special Publication (SP) 800-171Ar3 (Revision 3), *Assessing Security Requirements for Controlled Unclassified Information*. The goal of the primer is to help the small business community understand foundational SP 800-171 assessment concepts and basic strategies for planning for an assessment.

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 government-wide 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. CUI is marked by the federal agency, and it is the responsibility of the federal agency to ensure that requirements to protect CUI are identified in applicable contracts or agreements. Examples of CUI include:

	When provided as part of a government contract, examples include:	Marking [2]
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.

[1] *The security requirements in NIST SP 800-171 are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components.*

[2] *For more information on types of CUI and markings, visit the National Archives and Records Administration (NARA) https://www.archives.gov/cui.*

Audience

This primer is for business leaders or employees who are new to SP 800-171A and who are tasked with managing the implementation of SP 800-171, including conducting self-assessments or preparing to work with external assessors.

Key Terms:

Security Requirement [1]**:** Security outcomes levied on a nonfederal organization to ensure adequate measures are taken to protect the confidentiality of CUI being processed, stored, or transmitted.

Security Requirement Assessment
The testing or evaluation of security requirements to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

Definitions provided are intended as plain language. Review the NIST Glossary for official NIST definitions.

A Suite of Guidelines

NIST's suite of CUI guidelines (shown in the table below) focuses on protecting the *confidentiality*[3] of CUI in nonfederal systems and organizations and recommends specific security requirements to achieve that objective. **This guide will focus on SP 800-171A, Revision 3**.

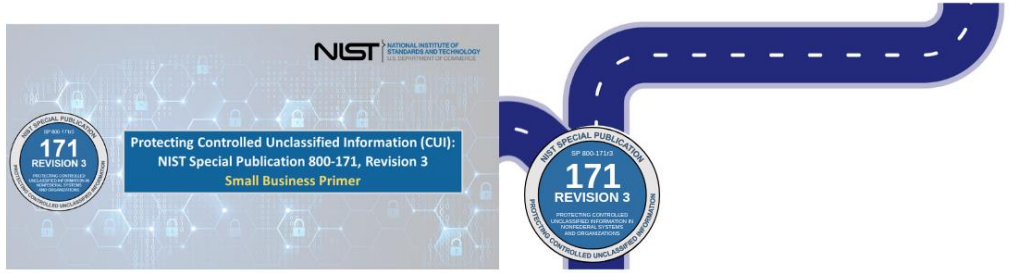
NIST SP 800-171 REVISION 3	NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems is a set of recommended security requirements for protecting the confidentiality of CUI.
NIST SP 800-171A REVISION 3	NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information **provides assessment procedures and a methodology to conduct assessments of the CUI security requirements in SP 800-171.**
NIST SP 800-172 REVISION 3	NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information provides enhanced security requirements to help protect CUI associated with critical programs or high value assets in nonfederal systems and organizations from the advanced persistent threat (APT). The SP 800-172 enhanced security requirements are designed to protect confidentiality, integrity and availability of information.
NIST SP 800-172A REVISION 3	NIST SP 800-172A, Assessing Enhanced Security Requirements for Controlled Unclassified Information provides assessment procedures and a methodology to conduct assessments of the enhanced security requirements in SP 800-172.

FAQ: Which version of SP 800-171 or SP 800-171A should I use?

At the time of this document's publication, the Department of War's Cybersecurity Maturity Model Certification (CMMC) Program leverages the requirements and assessment procedures in SP 800-171r2 (Revision 2) and SP 800-171Ar2.

Organizations can leverage the NIST-created change analysis (SP 800-171r2 to r3) to determine which revision best meets their current and future needs.

NIST SP 800-171,R3 Small Business Primer



Complementary Resource: NIST SP 800-171r3 Small Business Primer

The NIST SP 800-171r3 Small Business Primer is an awareness tool designed to help organizations make the leap to getting started with NIST SP 800-171r3. It provides:

- An overview of foundational components of SP 800-171
- A list of frequently asked questions and their answers
- Tips for getting started
- A brief introduction to each of the control families
- Related resources

[3] *SP 800-171 does not explicitly cover integrity and availability - so it is not a comprehensive security program. The enhanced security requirements SP 800-172 do address confidentiality, integrity, and availability.*

Assessing Security Requirements for CUI

The What and the How

Knowing ***what*** requirements to implement is important, but it is also important to understand ***how*** to evaluate the organization's implementation. Both publications work hand-in-hand.

Security Requirements ***(The What)***

Are We Effectively Implementing the Requirements? ***(The How)***

Who Conducts Assessments?

Assessments can be conducted by system developers, integrators, or owners; third-party assessors; or other staff members of the business.

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.

The security requirement assessment **process** gathers information and produces evidence to determine **how effectively the business (or organization) is protecting CUI** by:

Identifying potential problems or shortfalls in security and risk management programs	Identifying security weaknesses and deficiencies in systems and the environments in which those systems operate	Prioritizing risk mitigation decisions and activities	Confirming that identified security weaknesses and deficiencies in the system and environment of operation have been addressed	Supporting continuous monitoring activities and providing information security situational awareness

FAQ: Does NIST provide a list of recommended vendors to assist with implementation and assessment?

NIST does not endorse specific products or services. You may explore the CyberAB Marketplace* or MSPs for the Protection of Critical Infrastructure* to find and evaluate consulting firms who may assist in NIST SP 800-171 implementation.

**Non-NIST sites are included 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.*

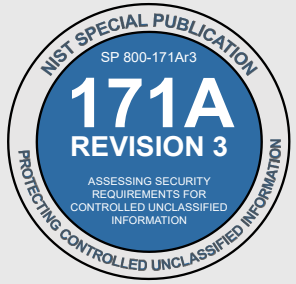
Roles Within the Ecosystem

NARA Determines What CUI Is

The National Archives and Records Administration (NARA), per 32 CFR Part 2002 "Controlled Unclassified Information," determines what CUI is and lists CUI types at archives.gov/cui

NIST Develops and Publishes the Security Requirements for the Protection of CUI

CUI Security Requirements



How to Assess the CUI Security Requirements

Voluntary Implementation and Assessment

Any organization may voluntarily implement the security requirements in SP 800-171 to help take appropriate measures to protect the confidentiality of sensitive information and then use SP 800-171A to assess the security requirements.

Federal Customer

The federal agency is responsible for communicating what CUI the business is responsible for protecting as part of the contractual arrangement. If there are questions, reach out to the contracting officer.

Required Implementation and Assessment

Federal and non-federal entities may require implementation and assessment of SP 800-171 (e.g., CMMC, SPRS). How requirements are mandated, and any compliance issues related to nonfederal implementation of SP 800-171, are the responsibility of the federal agency requiring its use, as expressed in a specific contract or agreement.

FAQ: What is the relationship between NIST and CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a DOW program that references the security requirements in NIST SP 800-171 and SP 800-172. NIST is not involved in the design, development, or implementation of the CMMC model, accreditation body, or certification process. It is important to note that CMMC is currently based on SP 800-171, Revision 2. Contractors should check for specific requirements in their contracts to understand which version they are required to use.

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.

All the SP 800-171Ar3 assessment objectives can be viewed in multiple formats (Excel, JSON, and online) with the Cybersecurity and Privacy Reference Tool.

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])*

Determination Statements

Each potential assessment objective includes a determination statement related to the security requirement. It's understood that there may be terminology in here that business leaders may be unfamiliar with. Most business leaders won't need to memorize this content. **The big picture on this page and page 8** is that these statements and identifiers help assessors trace each assessment activity back to a specific security requirement.

Determination Statement for Security Requirement

Makeup of Determination Statements:

- Each determination statement begins with the letter "A" to indicate that it is part of an assessment procedure.
- The next sequence of numbers or letters (e.g., 03.01.10) indicates the security requirement identifier from NIST SP 800-171 (and the specific control item if it is a multi-part requirement) that is the target of the assessment.
- Organization-defined parameters are indicated by the letters "ODP." If there are multiple ODPs in the determination statement, the ODP number is indicated in a square bracket (e.g., A.03.01.10.ODP[01]).
- Square brackets are also used to denote when an assessment procedure further decomposes a requirement into more granular determination statements (e.g., A.03.01.12.a[01], A.03.01.12.a[02], A.03.01.12.a[03]).

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)

Each determination statement within the Assessment Objective needs to be satisfied for a security requirement to be considered fully implemented.

Sample Security Requirement and Assessment Procedure

Below is an example of an SP 800-171 security requirement and its related SP 800-171A assessment procedure (color added for emphasis):

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)

Key Term

Organization-Defined Parameters (ODPs) are included in certain security requirements. It can be likened to a fill-in-the-blank exercise or declaring a variable when writing code. ODPs provide the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, operational environments, and risk tolerance.
ODPs support consistent security assessments in determining whether security requirements have been satisfied. For those in the Defense Industrial Base, the Department of War has assigned values for a subset of ODPs. NIST does not assign values to ODPs.

Ready, Set, Assess

Assessments determine the effectiveness of the safeguards implemented to protect CUI, the actions needed to manage security risks to the organization, and compliance with the security requirements.

Businesses can use the following pages to begin planning for an SP 800-171 self-assessment or for an external assessment. This primer provides businesses with a head-start on assessment preparation.

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

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. Whether planning to conduct a self-assessment or have an external assessment conducted, here are some tips for getting started:

Overview:

- ✓ Identify who will have responsibility for evaluating the business's implementation of the SP 800-171 security requirements. Does the business have the capability to do this in-house? Or is a third party needed to lead the assessment or to validate results from a self-assessment?
- ✓ Identify who within the business needs to be notified of the impending assessment.
- ✓ Identify what resources (e.g., time, financial, subject matter expertise, etc.) will be needed for the assessment.
- ✓ Identify the timeframe for the assessment. When does it need to start or be completed?
- ✓ **Appropriately scoping requirements** is an important factor in determining protection-related investment decisions and managing security risks for your business. Scope the assessment by identifying where CUI is stored, processed or transmitted. The security requirements in NIST SP 800-171 are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components.
  - ✓ Scope of the security requirements may be limited by isolating the system components in a separate security domain. Isolation can be achieved by implementing subnetworks with firewalls or other boundary protection devices. Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for CUI and avoid increasing the organization's security posture beyond what it requires for protecting its missions, operations, and assets.
- ✓ Review the System Security Plan, which describes the system boundary, the environment in which the system operates, how the security requirements are satisfied, and the relationships with, or connections to, other systems. This document is essentially your business' plan for meeting the security requirements of SP 800-171.
- ✓ **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. Whether planning to conduct a self-assessment or have an external assessment conducted, here are some tips for getting started:

Overview:

- ✓ 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.

- ✓ If available, gather:
  - Assessment results from previously accepted or approved assessments
  - Other cybersecurity assessment artifacts
  - These can be used as evidence for determining overall security requirement effectiveness.

- ✓ Review contracts or agreements for external systems that create, store, or transmit CUI.
  - The organization does not always have direct control over the security requirements used in external systems or sufficient visibility into the development, implementation, and assessment of those controls.
  - Review the contracts or agreements and tailor the assessment procedures as appropriate to assess the security requirements or the security requirement assessment results provided through contracts or agreements.

- ✓ Review the selected assessment procedures for the control families and combine or consolidate the procedures (or parts of procedures) whenever possible or practicable. Examples:
  - Obtain and examine configuration settings from similar hardware and software components within the system.
  - Consolidate interviews with key organizational officials who deal with a variety of security- or privacy-related topics.

Conducting the Security Requirement Assessment

After the assessment plan is approved by the business, the assessors execute the plan in accordance with the agreed-upon schedule. Assessment objectives are achieved by applying the designated assessment methods (examine, interview, test) to selected assessment objects and compiling or producing the evidence necessary to make the determination associated with each assessment objective.

Overview:

- ✓ The results of assessments are documented in assessment reports. Assessors produce one of the findings below for each determination statement contained within an assessment procedure:
  - **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.

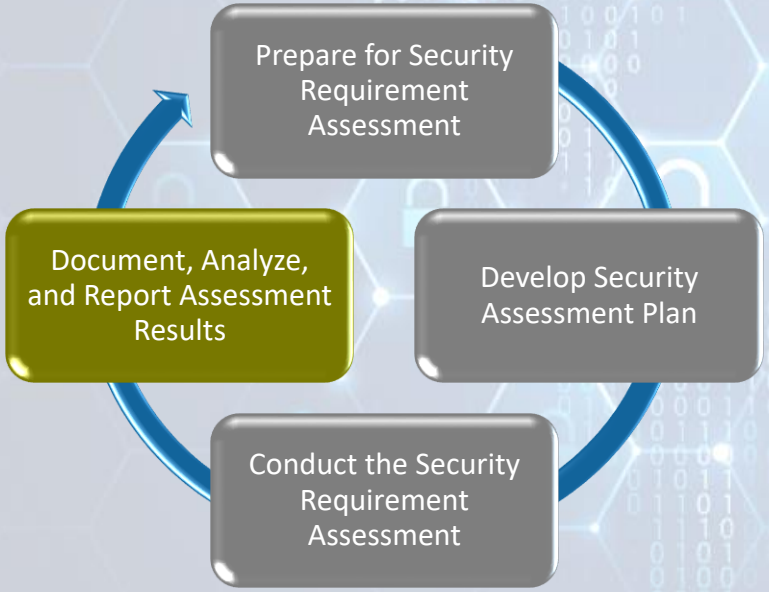
    Or
  - **Other than satisfied** – Indicates that the assessment objective for the requirement has not been met and has produced an unacceptable result. A finding of other than satisfied may also indicate that the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.
- ✓ **The goal of an assessment is to verify if the business is effectively implementing the requirements.** Not everyone speaks "cybersecurity," so assessors may consider asking clarifying questions during the assessment to help resolve ambiguity or assumptions.
- ✓ **During this phase, gaps might become apparent.** For example: what is documented in the System Security Plan might not actually be what is happening in practice, or policies exist but staff do not follow them. This gap analysis is critical for making improvements to how the business protects CUI.

? **FAQ: How do I get a "NIST SP 800-171 Assessment"?** 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.

Documenting, Analyzing, and Reporting Assessment Results

The assessment report includes information from assessors (in the form of findings) that is necessary to determine whether the security requirements in SP 800-171 have been satisfied. The report conveys the results of the assessment to and can also provide recommendations for correcting any deficiencies discovered during the assessment.

Documenting, Analyzing, and Reporting Assessment Results



Overview:

- The assessment report includes information from assessors that is necessary to determine whether the security requirements in SP 800-171 have been satisfied.
- Business leaders can then use insights from the findings to drive improvements (i.e., incorporate any gaps or issues from the security requirement assessment into a Plan of Action and Milestones).
- This is where businesses might also want to make improvements to their System Security Plan.
- It's also important to understand what requirements the business has for documenting and acting upon assessment results. For instance, is there a particular timeline for which the business needs to act upon assessment results? How do remediations need to be documented?
- **Learn More:** SP 800-53A Appendix E provides additional information on security assessment reports.
- **Learn More:** SP 800-18r2, *Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems.* This publication identifies essential elements of system plans from security, privacy, and cybersecurity supply chain risk management perspectives to promote consistent information collection across the organization, regardless of the system's mission or business function.

Additional Resources

FAQ: What are the SP 800-171A assessment procedures based on? The assessment procedures in SP 800-171A are based on and sourced to the assessment procedures in SP 800-53A. For additional information on preparing for security assessments, developing assessment plans, conducting assessments, and analyzing assessment report results, consult SP 800-53A.

Online Introductory Courses Available for the NIST SP 800-53 Series

SP 800-171 requirements are based on a subset of controls found in SP 800-53, which is a catalog of security and privacy controls for systems and organizations. With that in mind, it is important to have a basic understanding of the SP 800-53 series. **NIST has three self-guided online introductory courses** providing a high-level overview of foundational security and privacy risk management concepts.

The online introductory courses are between 45-60 minutes, are available at no cost, and registration is not required. Access the courses.

Additional Resources

- NIST's Protecting CUI Frequently Asked Questions
- Changes Between SP 800-171 Rev. 2 and Rev. 3 (.xlsx)
- The NIST Cybersecurity and Privacy Reference Tool (CPRT)
- "CUI Security Requirements Workshop" (event recording)
- NIST Small Business Cybersecurity Corner
- Defense Industrial Base Sector Coordinating Council Cyber Assist
- Manufacturing Extension Partnership