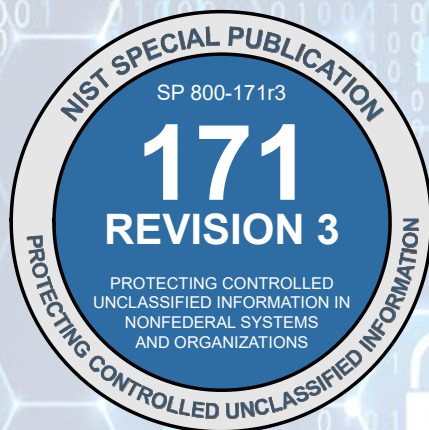




Check for
updates



Protecting Controlled Unclassified Information (CUI): NIST Special Publication 800-171, Revision 3 **Small Business Primer**

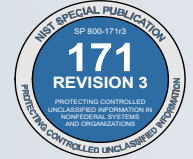
U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
*Craig Burkhardt, Acting Under Secretary of Commerce for Standards and
Technology and Acting NIST Director*

**NIST Special Publication
NIST SP 1318**

<https://doi.org/10.6028/NIST.SP.1318>
August 2025

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.		

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

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.

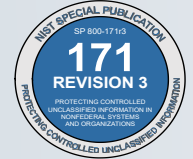
Key Term: Confidentiality



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"](#).

Overview



A Suite of Guidance

NIST's suite of CUI guidance (shown in the table below) focuses on protecting the **confidentiality**² of CUI in nonfederal systems and organizations and recommends specific security requirements to achieve that objective. **This guide will focus on 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, 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, 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, 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.

Key Term: Security Requirement

[SP 800-171] Security Requirement: Security outcomes levied on a nonfederal organization to ensure adequate measures are taken to protect the confidentiality of CUI being processed, stored, or transmitted.

Important Note: 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.

A is for Assessment

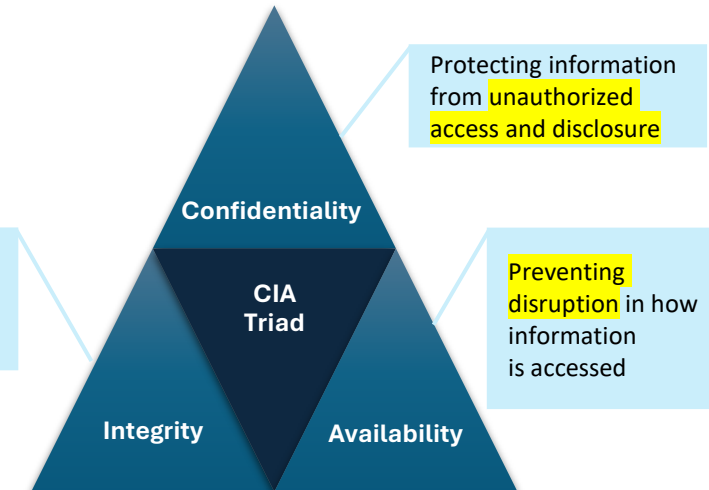
Knowing what requirements to implement is important, but it is also important to understand **how** to evaluate the organization's implementation. Both publications work hand-in-hand for full implementation.



Recommended Requirements

Are We Effectively Implementing the Requirements?

Protecting information from **unauthorized modification**



² SP 800-171 does not explicitly cover integrity and availability - so it is not a comprehensive security program.

Overview

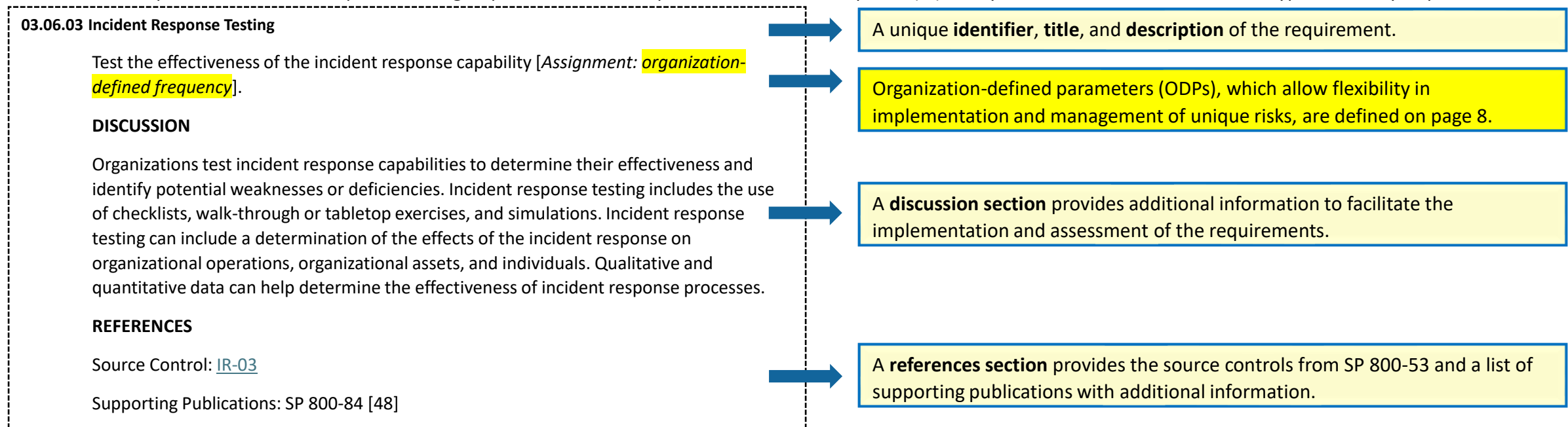
Structure of SP 800-171

SP 800-171 security requirements are organized into 17 families, as illustrated in the table below. Each family is further broken down into requirements related to the family's general security topic (see the example at the bottom of the page).

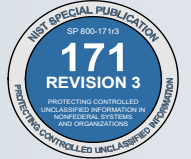
Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

Understanding the Security Requirements in SP 800-171

Below is an example of the Incident Response Testing requirement, which is part of the Incident Response (IR) family. The structure and content of a typical security requirement includes:




Top 5 Frequently Asked Questions



Top five questions NIST receives on SP 800-171:

How can I “comply” with SP 800-171?	<i>NIST does not have a role in determining compliance with the security requirements in SP 800-171. If you have questions regarding requirements to protect CUI or other regulatory requirements, please contact your prime contractor and/or federal point of contact for the contract.</i>
How do I know if I have CUI?	<i>It is the responsibility of the federal agency to ensure that requirements to protect CUI are identified in applicable contracts or agreements, and CUI is marked by the federal agency.</i>
How do I get a “NIST SP 800-171 Assessment”?	<p><i>The term “NIST Assessment” and “NIST SP 800-171 Assessment” is frequently used to describe the Department of Defense (DOD) process used to complete its NIST SP 800-171 Assessment Module through the Supplier Performance Risk System (SPRS).</i></p> <p><i>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 DOD’s implementation of its programs. For additional guidance on NIST’s methodology to plan, prepare for, and conduct security requirement assessments, refer to SP 800-171A.</i></p>
What products, vendors, or solutions are “NIST SP 800-171 compliant” or “CMMC-certified”?	<i>NIST does not identify or track implementation of or compliance with the security requirements.</i>
What is the relationship between NIST and CMMC?	<i>The Cybersecurity Maturity Model Certification (CMMC) is a DOD 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.</i>

 [View more FAQs here.](#)



If you still have a question after reviewing all our FAQs, send your question to: sec-cert@nist.gov.

Additional Resources

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



SP 800-171 requirements are focused on protecting confidentiality and 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. To assist, **NIST has released three self-guided online introductory courses** to provide 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.](#)

Roles of Different Federal Agencies

- 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](https://www.archives.gov/cui).
- **NIST** is responsible for developing and publishing the security requirements for the protection of CUI. **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.

Additional NIST 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 \(CPRT\)](#) provides online, interactive versions of the updated security requirements in SP 800-171, Revision 3 and the updated assessment procedures in SP 800-171A, Revision 3
- Event Recording: "[CUI Security Requirements Workshop](#)," which provides a general overview of SP 800-171 and SP 800-171A
- [NIST Small Business Cybersecurity Corner](#)

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:



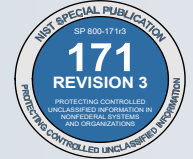
Page 8: Key differences between SP 800-171 R2 and R3.

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.

What's New in SP 800-171, Revision 3?



SP 800-171, Revision 3 was published in May 2024. Significant changes include:

Updates to the Security Requirements and Families

- Based on [NIST SP 800-53, Revision 5](#) and the [NIST SP 800-53B](#) moderate impact control baseline.
 - Applies updated tailoring criteria addressing stakeholder feedback (adding new, consolidating, and withdrawing requirements).
- Includes increased specificity in security requirements.
- Introduces organization-defined parameters (ODP) to increase flexibility to better manage organization-specific risks.

Additional Revision 3 Resources

- A [CUI overlay](#) (.xlsx) showing the direct link between SP 800-53 and SP 800-171, including NIST's tailoring decisions.
- Transitioning your organization from implementation of Revision 2 to Revision 3? Review this detailed analysis of the [changes between Revision 2 and Revision 3](#) (.xlsx).
- The SP 800-171 security requirements in multiple formats (Excel, JSON, and online) through the [NIST Cybersecurity and Privacy Reference Tool](#).

Key Terms

Control Baseline: A set of controls you can implement to meet strategic, legal, regulatory, or contractual security and privacy requirements and manage risk.

Organization-Defined Parameters (ODPs) are included in certain security requirements. 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. If a federal agency or a consortium of agencies do not specify a particular value or range of values for an ODP, nonfederal organizations must assign the value or values to complete the security requirement.

Tailoring: The process by which control baselines are modified to achieve certain organizational goals and objectives.

Definitions provided are intended as plain language. Review the [NIST Glossary](#) for official NIST definitions.

General Tips for Getting Started with NIST SP 800-171

Everyone will have different approaches to getting started, but here are a few tips to get you started down the right path:

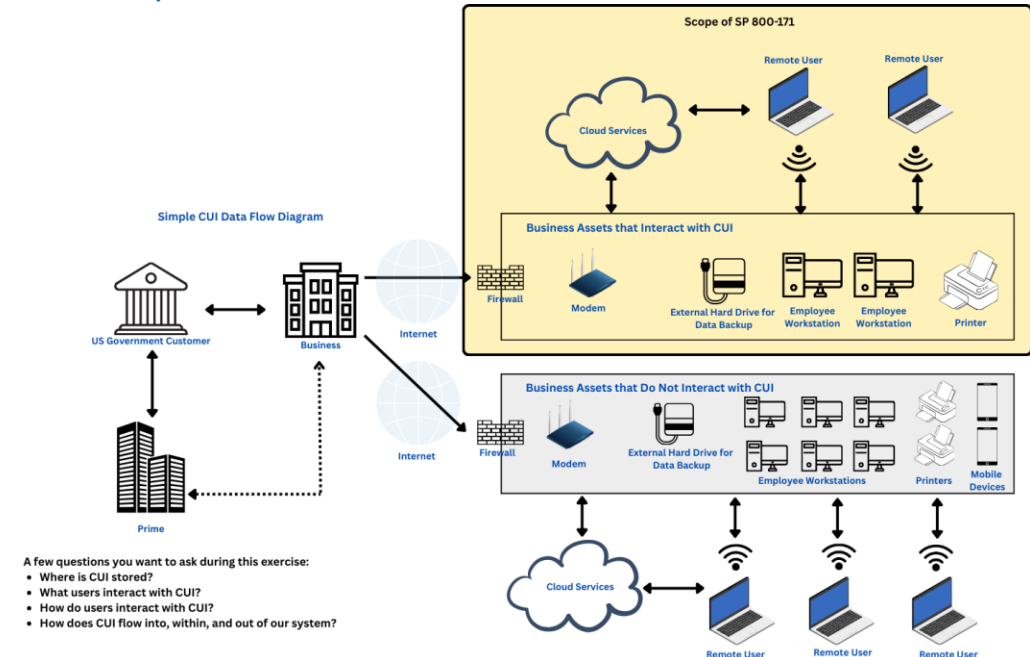
Determine if your business has CUI.

Understand current (or future) legal, regulatory, or contractual requirements for protecting CUI. 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. The business may also have additional compliance requirements beyond SP 800-171. If so, an initial task might be to understand where the requirements overlap and where they differ. With that information, the business can begin addressing requirements that meet multiple compliance requirements.

Understand how CUI flows into, within, and out of the business.

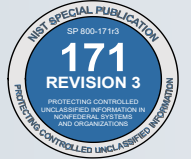
Inventorying what systems or components the business has, and how the data flows into, within, and out of those systems or components, helps practitioners understand the scope of applicability of SP 800-171 security requirements to business systems.

Below is a sample CUI data flow diagram for a fictional company. Create your own diagram to understand how CUI flows into, within, and out of the business.



Scope and Applicability of SP 800-171. 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. **Appropriately scoping requirements is an important factor in determining protection-related investment decisions and managing security risks for your business.** You may limit the scope of the security requirements 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.

General Tips for Getting Started with NIST SP 800-171



Identify the role(s) responsible for security and provide the necessary resources.	Whether it is just one person or multiple people within the business, ensure roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced. Even if cybersecurity activities are outsourced to an external provider, someone within the business should still be designated to manage cybersecurity risk.
It's not all technology.	An important point to emphasize is that many requirements in SP 800-171 do not need investments in technology or services to implement. Many requirements can be achieved through the creation of processes and procedures.
Implement the requirements and document implementation in a system security plan.	Satisfying the security requirements won't be accomplished overnight. Implement in phases based upon your resources (including time, expertise, budget, etc.), starting with understanding what security requirements you may have already satisfied and building from there. A system security plan documents how an organization meets or plans to meet the security requirements for a system. In particular, the system security plan 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. View sample templates for system security plans on the Defense Industrial Base Sector Coordinating Council website.
Create a plan of action and milestones (POAM).	Once you have completed your audit or security assessment, describe how unsatisfied security requirements will be met and how planned mitigations will be implemented. Organizations can create system security plans and POAMs as separate or combined documents in any format. Federal agencies may consider system security plans and POAMs as inputs to risk-based decisions on whether to process, store, or transmit CUI on a system hosted by a nonfederal organization. View an editable template .
Find help when you need it.	Consider reaching out to a local Manufacturing Extension Partnership or APEX Accelerator to help you get started. Regularly communicate with your prime contractor or contract officer to understand contract requirements. Decide if you need to increase the skills of your existing staff, hire new people, or engage an external partner to help you. If hiring an external partner, such as a managed security services provider (MSSP), talk to others in your industry to get their perspective on vendors they have worked with and always thoroughly review any contract or agreement prior to signing. A helpful resource, assembled by member company participants of the National Defense Information Sharing & Analysis Center (ND-ISAC), is the Defense Industrial Base Managed Service Provider Shopping Guide for Small & Medium-Sized Businesses . You may also explore the CyberAB Marketplace to find a consulting firm to assist in NIST 800-171 implementation.*
Review NIST SP 800-171A to help you understand how the security requirements in SP 800-171 can be self-assessed or are assessed by independent, third-party entities or by the government.	

*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.

Getting Started with Access Control

Family: Access Control

Description: Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.*

Getting Started with Access Control



Implement policies and procedures that limit access to CUI on systems and devices **to only those individuals that require such access to do their jobs.**

Complete a review of publicly available information, such as information on the company website.

- ✓ Review the content for CUI and remove such information if discovered. CUI should not be available to the public.

Protect CUI with device locks and session termination.

- ✓ Train staff on these behaviors and establish policies that prevent unauthorized individuals from seeing CUI or other sensitive information on a device while the device is unattended by an individual. When the individual returns to their device, they will have to re-establish access by using a password or biometric authenticator

Foundational Concept—Least Privilege: This involves limiting access rights to only those users who need it to accomplish assigned tasks.

- Identify who has access to CUI and the system. Only those who require access to CUI should have it. For example, if a network or system administrator does not need access to CUI, their access should be restricted.
- Reassign or remove privileges as necessary, such as when an individual no longer requires access to CUI and the system.
- Identify who within the business has administrative (i.e., system administrator or domain administrator) privileges on systems and devices. Limit administrative privileges to only those who need them to perform specified tasks. Implement policies that restrict use of these accounts for routine, day-to-day tasks that do not require administrative privileges.

Related Resources:

- [View all SP 800-171 Access Control Requirements and Assessment Procedures](#)
- [NIST Identity and Access Management Resources](#)

**Family definitions, except for "Supply Chain Risk Management," are adapted from FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.*

Getting Started with Awareness and Training

Family: Awareness and Training

Description: Ensuring personnel are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, regulations, or procedures related to the security of organizational systems; and ensuring that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Getting Started with Awareness and Training



Regularly provide basic and advanced security literacy training to new and existing staff. Customize the content to make it relevant—based on the systems that personnel have authorized access to, contextualized to the work environments of personnel (e.g., telework, shop floor), and tailored to the specific roles of personnel. The content should include:

- ✓ An understanding of the need for security (why is cybersecurity important to our business mission?).
- ✓ Specific actions required of users to maintain security (required use of multi-factor authentication, not sharing passwords, etc.).
- ✓ How to respond to confirmed or suspected incidents.
- ✓ How to securely handle CUI (training should be provided to staff before authorizing access to the system or CUI).
- ✓ How to recognize and report [insider threats](#), [social engineering](#), and [social mining](#).

Examples of security awareness techniques include displaying posters, offering supplies inscribed with security reminders, generating email advisories or notices from leadership, and conducting awareness events—such as a lunch-and-learn or workshop.

There are many resources that are free and open to the public that can be incorporated into awareness and training, such as videos, online courses, and awareness posters. The resources will likely need to be customized to meet your own unique business needs, but they offer a starting point. Resources can be found in the resources box below.

Related Resources:

- [View all SP 800-171 Awareness and Training Requirements and Assessment Procedures](#)
- [NARA CUI training](#)
- [NIST Free and Low-Cost Online Cybersecurity Learning Content](#)
- [Center for Development of Security Excellence Security Awareness Hub](#)

Getting Started with Audit and Accountability

Family: Audit and Accountability

Description: Creating, protecting, and retaining system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity; and ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Getting Started with Audit and Accountability



Understand and track who is performing actions within business system(s), what those actions are, and when those actions are taken. Having the ability to review system activity and analyze records, generate reports, resolve audit log process failures, and protect audit data gives the business insight into potential unauthorized activity and improves the ability to respond quickly and appropriately. Consider automated tools for conducting audit and logging activities. Products range from free, open-source tools to commercially available ones.

Define, maintain, and protect audit record content.

- ✓ Ask internal information security staff, or your security vendor, what audit log information, if any, the system currently captures and how it is protected and maintained.

Questions to Ask:

- Do audit records contain information that establishes type of event, when the event occurred, where the event occurred, the source of the event, outcome, and the identity of the individual associated with the event?
- Who within the business should be alerted when there are, for instance, software and hardware errors, failures in audit log capturing mechanisms, or reaching or exceeding audit log storage capacity?
- Are we retaining audit records for a period consistent with the business records retention policy? Note that some industries and types of data (e.g., financial, employee, and medical records) have regulatory specifications.
- How are audit information and audit logging tools being protected from unauthorized access, modification, and deletion?
- Is access to management of audit logging functionality authorized to only a subset of privileged users or roles?
- How frequently are these records reviewed?

Related Resources:

- [View all SP 800-171 Audit and Accountability Requirements and Assessment Procedures](#)
- [Logging Made Easy, Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
- [NIST Log Management resources](#)

Getting Started with Configuration Management

Family: Configuration Management

Description: Establishing and maintaining baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation); and establishing and enforcing security configuration settings for information technology products employed in organizational systems.

Getting Started with Configuration Management



Changes to a system can have potentially significant effects on the security of the system. Configuration management helps establish processes for initializing, changing and monitoring configurations to the hardware, software, or firmware components of the system or the operational procedures related to the system storing CUI.

Limit who can make changes to the system containing CUI.

- ✓ Permit only qualified and authorized individuals to access the system for the purpose of initiating changes. Access restrictions include physical and logical access controls, software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into the system), and change windows (i.e., changes occur only during specified times).

Authorized software – allow by exception.

- ✓ It is important to identify permitted and prohibited actions regarding software installation when users have the ability to install software on organizational systems. Permitted software installations could include updates and security patches to existing software and downloading new applications from organization-approved “app stores.” Companies might prohibit employees from downloading certain programs, services, software versions, etc.

Locate CUI.

- ✓ Identify the location of CUI and the system components on which the information is processed and stored. Identify who within the business has access to CUI. Again, remember to restrict this access to only those who need it.

Foundational Concept– Least Functionality: Systems (databases, email systems, network drives, etc.) provide a variety of functions and services. Some functions and services that are routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Configure the system to provide only mission-essential capabilities. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

Related Resources:

- [View all SP 800-171 Configuration Management Requirements and Assessment Procedures](https://csrc.nist.gov/projects/protecting-controlled-unclassified-information)

Getting Started with Identification and Authentication

Family: Identification and Authentication

Description: Verifying the identity of a user, process, or device, as a prerequisite to allowing access to resources in a system.

Getting Started with Identification and Authentication



To protect your business from fraud and unauthorized system and data access, you want to take steps to ensure that only the right people and technologies have the right level of access to the right resources at the right time.

Enable Multi-Factor Authentication (MFA)— For many busy small business owners, the use of passwords has been the primary method for locking down access to sensitive systems and data. However, passwords alone are not effective for protecting your data from most attackers. They have become too easy for threat actors to exploit at scale and with limited effort. MFA is an important security enhancement that requires a user to verify their identity by providing more than just a username and password. It requires a user to provide a combination of two or more of the following:

Something you know:	Such as a PIN or password.
Something you have:	Such as a smart card or security key.
Something you are:	Such as a fingerprint or face.

Implement MFA for access to privileged and non-privileged accounts. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level to provide increased security.

Maintain strong password management.

- ✓ Define password rules for your organization.
- ✓ When you send passwords to others, do so using cryptographically protected forms, such as through encrypted email or password managers.
- ✓ Maintain a list of commonly used, expected, or compromised passwords, and update the list regularly. Verify your passwords are not found on the list when users create or update passwords.

Related Resources:

- [View all SP 800-171 Identification and Authentication Requirements and Assessment Procedures](#)
- [NIST Identity and Access Management Resources](#)
- [NIST Small Business Cybersecurity Corner: Multi-Factor Authentication](#)
- [Require Strong Passwords, CISA](#)

Getting Started with Incident Response

Family: Incident Response

Description: Establishing an incident handling capability for systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and tracking, documenting, and reporting incidents to appropriate organizational officials and/or authorities.

Getting Started with Incident Response



It is important that organizations develop and implement a coordinated approach to incident response. Before an incident occurs, be ready with a basic response plan. This will be customized based on the business, but should include:

- ✓ A business champion: Someone who is responsible for developing and maintaining the incident response plan.
- ✓ Who to call: List all the individuals who may be part of the incident response efforts. Include their contact information, roles, and responsibilities.
- ✓ What/when/how to report: List the business' communications/reporting responsibilities as required by laws, regulations, contracts, agreements, or policies.
- ✓ Also, most federal contracts will include specific reporting and notification requirements that should be included in the Incident Response Plan

Contact	Phone	Email	Role	Responsibility
Business Leader				
Technical Contact				
State Police				
Local FBI Representative				
Bank Contact				
Legal Contact				
Insurance Contact				

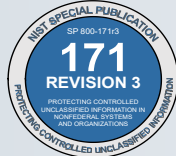
This table is an example and is not exhaustive. Organizations will likely have additional or alternative contacts to add to this table.

Related Resources:

- [View all SP 800-171 Incident Response Requirements and Assessment Procedures](#)
- [NIST Incident Response Project](#)

- [Incident Response Plan Basics, CISA](#)


Getting Started with Maintenance



Family: Maintenance

Description: Performing periodic and timely maintenance on organizational information systems; and providing effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Getting Started with Maintenance

 All systems need regular maintenance, such as hardware or software updates. Without this maintenance, the systems are vulnerable to cybersecurity risks—potentially exposing CUI or other sensitive information. It is important that authorized individuals perform regular maintenance following established procedures to protect the business, systems, and data.

Have a Maintenance Plan <ul style="list-style-type: none">✓ Identify the tools that are used for diagnostic and repair actions on the system.✓ Determine a regular maintenance schedule and build in mechanisms to verify it is followed.✓ Track regularly scheduled maintenance and any emergency repairs.✓ Enable automatic updates where appropriate.✓ Plan for upgrades to end-of-life hardware or software that will no longer be supported.	Maintenance Personnel – refers to individuals who perform hardware or software maintenance on the system. <ul style="list-style-type: none">✓ Identify the individuals or organizations who are authorized to perform hardware or software maintenance on the system. Consider issuing temporary credentials to external parties, which may be for one-time use or for very limited time periods.
Nonlocal Maintenance – Organizations might need to have maintenance performed on systems by someone who is not physically on site. <ul style="list-style-type: none">✓ Ensure a maintenance session with an authorized provider is established.✓ Ensure multi-factor authentication is enabled when establishing the maintenance session.✓ Fully terminate the connection when the maintenance is complete.	Prevent the removal of system maintenance equipment containing CUI <ul style="list-style-type: none">✓ Verify that there is no CUI on the equipment by sanitizing or destroying the equipment or retaining the equipment within the facility before it is removed.

Related Resources:

- [View all SP 800-171 Maintenance Requirements and Assessment Procedures](#)
- [Understanding Patches and Updates, CISA](#)
- [NIST Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology](#)

Getting Started with Media Protection

Family: Media Protection

Description: Protect system media, both paper and digital; limiting access to data on system media to authorized users; and sanitizing or destroying system media before disposal or release for reuse.

Getting Started with Media Protection



Media includes both digital and non-digital media (e.g., flash drives, external or removable drives, or paper).

Physically control and securely store system media that contain CUI.

- ✓ Conduct an inventory of what media contains CUI.
- ✓ Establish procedures to allow authorized individuals to check out and return physical media to designated areas.
- ✓ Securely store media (e.g., locked drawer, desk, cabinet, or a controlled media library).
- ✓ Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.
- ✓ Sanitize media. If media is designated for disposal or reuse—such as transitioning a device to a different employee or it is being donated to a community non-profit, CUI will need to be removed from media such that the information cannot be retrieved or reconstructed.

Restrict access to CUI on media to authorized personnel or roles.

- ✓ Understand who has access to digital and physical media. Periodically review to modify or remove access, as appropriate.

Maintaining accountability of media during transport.

- ✓ Restrict transport activities to authorized personnel. Track or obtain the records of transport activities as the media move through the transportation system to prevent and detect loss, destruction, or tampering.

Related Resources:

- [View all SP 800-171 Media Protection Requirements and Assessment Procedures](#)
- [NIST Guidelines for Media Sanitation](#)
- [Protecting Data on Old Devices You Don't Use Anymore, CISA](#)
- [CUI Marking Job Aid, DCSA](#)

Getting Started with Personnel Security

Family: Personnel Security

Description: Ensuring that individuals (including third-party service providers) are trustworthy and meet established security criteria for those positions; ensuring that organizational information and systems are protected during and after personnel actions such as terminations and transfers; and employing formal sanctions for personnel failing to comply with organizational security policies and procedures.

Getting Started with Personnel Security



Personnel security screening activities involve the assessment of the conduct, integrity, judgment, and reliability of an individual (i.e., the individual's trustworthiness) **prior to authorizing access to the system or when elevating system access**. The screening and rescreening activities reflect applicable federal laws, directives, policies, regulations, and criteria established for the level of access required for the assigned position.

Establish a process for screening individuals prior to authorizing access to the system, such as utilizing background checks.

Establish policies and procedures for personnel termination.

- ✓ Disable system access.
- ✓ Terminate or revoke authenticators and credentials associated with the individual.
- ✓ Retrieve system property.

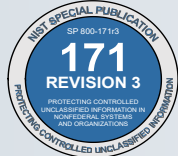
Establish policies and procedures for personnel reassignment or transfer.

- ✓ Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility.
- ✓ Modify access authorization to correspond with any changes in operational need.

Related Resources:

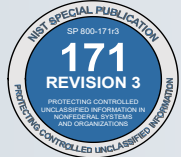
- [View all SP 800-171 Personnel Security Requirements and Assessment Procedures](#)
- [Resources for Onboarding and Employee Screening, CISA](#)

Getting Started with Physical Protection



Family: Physical Protection	
Description: Limiting physical access to systems, equipment, and the respective operating environments to authorized individuals; protecting the facility and support infrastructure for systems; providing supporting utilities for systems; protecting systems against environmental hazards; and providing appropriate environmental controls in facilities containing systems.	
Getting Started with Physical Protection	
Physical Access Authorizations <ul style="list-style-type: none">✓ Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.✓ Issue authorization credentials (i.e., identification badges, identification cards) for employee and visitor facility access.✓ Periodically review the facility access list.✓ Remove individuals from the facility access list when access is no longer required.	Enforce Physical Access Authorizations – (e.g., monitors, printers, scanners) to prevent unauthorized individuals from accessing CUI. <ul style="list-style-type: none">✓ Place these devices in locked rooms or other secured areas with keypad or card reader access controls.✓ Only allow access to authorized individuals.✓ Place output devices in locations that can be monitored.✓ Use privacy screens on monitors to prevent unauthorized individuals from seeing sensitive data.
Alternate Work Sites – Determine alternate work sites that are allowed for use by employees (e.g., private residences, coworking spaces). <ul style="list-style-type: none">✓ Identify approved alternate work sites.✓ Establish security requirements for that site.	Enforce Physical Access Authorizations – such as entry and exit points of physical locations. <ul style="list-style-type: none">✓ Use control systems such as card readers, keys, locks, or guards.✓ Escort visitors and control visitor activity, such as limiting what areas of your facility they may visit.
Monitor Physical Access – of any physical locations containing systems or system components that process, store, or transmit CUI. Physical access monitoring includes publicly accessible areas within organizational facilities. <ul style="list-style-type: none">✓ Examples of physical access monitoring include guards, visitor logs, video surveillance equipment (i.e., cameras), and sensor devices.	
Related Resources: <ul style="list-style-type: none">• View all SP 800-171 Physical Protection Requirements and Assessment Procedures• The Power of Hello, CISA	

Getting Started with Risk Assessment



Family: Risk Assessment

Description: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of organizational information.

Getting Started with Risk Assessment



It is critical to periodically assess the associated risks to systems that create, process, store, or transmit CUI. Risk assessments consider threats, vulnerabilities, likelihood, and adverse impacts to organizational operations and assets based on the operation and use of the system and the unauthorized disclosure of CUI. Risk assessments also consider risks from external parties (e.g., contractors operating systems on behalf of the organization, service providers, individuals accessing systems) and include supply chain-related risks associated with suppliers or contractors and the system, system component, or system service that they provide.

Convene a team of individuals from across the organization (also include any vendors or contractors) to:

- ✓ Inventory all systems, data, and physical assets that process, store, or transmit CUI: where is our CUI? Include those also used by third party vendors or contractors.
- ✓ Identify the risks (internal and external threats and vulnerabilities, likelihood of occurrence and overall impact) associated with each asset. For example,
 - *Product design specifications are accessed by an unauthorized individual.*
 - *A contractor’s credentials to systems containing CUI are compromised.*
 - *Loss of access to financial systems.*
- ✓ Once assets are identified, categorize each based on the impact to the organization if the confidentiality of the CUI were to be compromised. For example, assign a “high, moderate, or low” impact rating for each.

Periodic Vulnerability Monitoring

- ✓ Establish a frequency at which the system containing CUI is monitored and scanned for vulnerabilities. Include all systems and system components that process, store, or transmit CUI (networks, services, printers, copy machines).
- ✓ Establish a policy that directs if vulnerabilities are discovered, they are remediated as quickly as possible.
- ✓ Many small businesses might not have the resources to conduct risk assessments or vulnerability monitoring and remediation. If this is the case, consider engaging a vendor who can be your partner in risk management.

Related Resources:

- [View all SP 800-171 Risk Assessment Requirements and Assessment Procedures](#)
- [NIST SP 800-30, Guide for Conducting Risk Assessments](#)

Getting Started with Security Assessment and Monitoring

Family: Security Assessment and Monitoring

Description: Periodically assess systems to determine if the requirements are effective; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in systems; and monitor requirements on an ongoing basis to ensure their continued effectiveness.

Getting Started with Security Assessment and Monitoring



By periodically assessing the security requirements, organizations determine whether the requirements are implemented correctly, operating as intended, and producing the desired outcome. Security assessments identify weaknesses in the system and provide the essential information needed to make risk-based decisions. These can be self-assessments or can be completed by a third party.

Develop a Plan of Action and Milestones (POAM)– Once an audit or assessment is completed, describe how unsatisfied security requirements will be met and how planned mitigations will be implemented within a POAM. Organizations can create POAMs in any format. Federal agencies may consider POAMs as inputs to risk-based decisions on whether to process, store, or transmit CUI on a system hosted by a nonfederal organization.

Weaknesses	Responsible Office/Organization	Resource Estimate (Funded/Unfunded /Reallocation)	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	How Was the Weakness identified?	Status (Ongoing or Complete?)

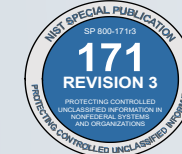
[View an editable template.](#)

Continuous Monitoring– Continuous monitoring at the system level facilitates ongoing awareness of the system security posture to support risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their systems at a frequency that is sufficient to support risk-based decisions. Different types of security requirements may require different monitoring frequencies. There are commercially available tools to help businesses achieve continuous monitoring or third-party vendors can support continuous monitoring goals.

Related Resources:

- [View all SP 800-171 Security Assessment and Monitoring Requirements and Assessment Procedures](#)
- [FedRAMP POAM Template \(.xlsx\)](#)

Getting Started with System and Communication Protection



Family: System and Communication Protection

Description: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of the systems; and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Getting Started with System and Communication Protection

Protect Your (System) Boundary

- ✓ Know what is coming and going across business systems. Communications at external and key internal managed interfaces of the system, such as gateways, routers, firewalls, and encrypted tunnels are monitored and controlled.
- ✓ Protect internal networks from publicly accessible ones by setting up subnetworks – physically or logically separated parts of the network – to separate them.
- ✓ Protect the system from external system connections by only allowing connections through managed interfaces.
- ✓ Deny network communications traffic by default. Only allow network communications traffic by exception.
- ✓ Terminate the network connections at the end of the session or after a defined period of inactivity.

CUI Transmission and Storage Confidentiality

- ✓ Encryption is a process of protecting your data so that only those authorized and equipped with a method to unencrypt the data (such as with an encryption key) can view it.
- ✓ Encryption protects CUI from unauthorized disclosure during transmission and while in storage.
- ✓ Mechanisms that protect the confidentiality of CUI during transmission include TLS and IPsec.
- ✓ Securely store your encryption key(s) so that you do not lose access to your systems or assets.
- ✓ There are many free and paid encryption tools available.

Related Resources:

- [View all SP 800-171 System and Communications Protection Requirements and Assessment Procedures](#)
- [NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices](#)
- [NIST Guidelines for the Selection, Configuration, and Use of Transport Layer Security \(TLS\) Implementations](#)
- [How to Protect Data that is Stored on Your Devices, CISA](#)

Getting Started with System and Information Integrity

Family: System and Information Integrity

Description: Identify, report, and correct information and system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational systems; and monitor system security alerts and advisories and take appropriate actions in response.

Getting Started with System and Information Integrity



Staying up to date on system security alerts, advisories, and directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations. There are many publicly available sources of system security alerts and advisories, including:

➡ [The Cybersecurity and Infrastructure Security Agency \(CISA\)](#)

➡ [National Security Agency \(NSA\)](#)

➡ [Federal Bureau of Investigation \(FBI\)](#)

➡ Software vendors, subscription services, and industry Information Sharing and Analysis Centers (ISACs) may also provide security alerts and advisories.

Establish a System Monitoring Strategy, Including:

- ✓ Procedures for system monitoring tools and techniques.
- ✓ Monitoring the system to detect attacks, indicators of potential attacks, and unauthorized connections.
- ✓ Detection of unauthorized use of the system.
- ✓ Unusual or unauthorized activities or conditions for inbound communications traffic.
- ✓ Unusual or unauthorized activities or conditions for outbound communications traffic.

Information Management and Retention:

- ✓ Establish policies and procedures for managing and retaining CUI in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
- ✓ Retaining CUI on nonfederal systems after contracts or agreements have concluded increases the attack surface for those systems and the risk of the information being compromised.

Related Resources:

- [View all SP 800-171 System and Information Integrity Requirements and Assessment Procedures](#)
- [NIST Ransomware Protection and Response](#)
- [Detecting a Potential Intrusion, CISA](#)

Getting Started with Planning

Family: Planning

Description: Develop, periodically update, and implement security plans for organizational systems that describe the security measures in place or planned for the systems and the rules of behavior for individuals accessing the systems.

Getting Started with Planning



Develop and disseminate to personnel the policies and procedures needed to satisfy the security requirements for the protection of CUI. Periodically review and update policies and procedures. Policy and procedures contribute to security assurance and enables consistent implementation of the business' risk management strategy.

Develop a System Security Plan That:

- ✓ Defines the system components;
- ✓ Identifies the information types processed, stored, and transmitted by the system;
- ✓ Describes specific threats to the system that are of concern to the organization;
- ✓ Describes the operational environment for the system and any dependencies on or connections to other systems or system components;
- ✓ Provides an overview of the security requirements for the system;
- ✓ Describes the safeguards in place or planned for meeting the security requirements;
- ✓ Identifies individuals who fulfill system roles and responsibilities; and
- ✓ Includes other relevant information necessary for the protection of CUI.

Periodically review and update the system security plan and take steps to protect it from unauthorized disclosure.

Rules of Behavior:

- ✓ Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.
- ✓ Provide rules to individuals who **require** access to the system.
- ✓ Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.
- ✓ Periodically review and update the rules of behavior, as needed.

Related Resources:

- [View all SP 800-171 Planning Requirements and Assessment Procedures](#)
- [Sample Templates for System Security Plans, DIB Sector Coordinating Council Industry Task Force](#)
- [FedRAMP Documents and Templates](#)

Getting Started with System and Services Acquisition

Family: System and Services Acquisition

Description: The allocation of sufficient resources to adequately protect organizational systems; employing system development life cycle processes that incorporate information security considerations; employing software usage and installation restrictions; and ensuring that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

Getting Started with System and Services Acquisition



Assessing the security of systems and services before acquisition and throughout the operational life of the system or service is critical for reducing your risks and adequately protecting organizational information systems.

Unsupported System Components:

- ✓ Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts.
 - *An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in opportunities for adversaries to exploit weaknesses or deficiencies components.*
- ✓ Establish procedures for the replacement or continued use of unsupported system components.
- ✓ Justify use of continued use of unsupported system components and determine risk mitigation options or identify alternative sources for continued support.
 - *Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities when newer technologies are unavailable or when the systems are so isolated that installing replacement components is not an option.*

External System Services:

- ✓ Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges.
- ✓ **The responsibility** for managing risks from the use of external system services remains with the business charged with protecting CUI.
- ✓ Review new or existing service level agreements for the following criteria:
 - Security requirements to be satisfied by external system service providers are defined.
 - Roles and responsibilities are clearly defined.
 - A description of measurable outcomes.
 - Remedies, mitigations, and response requirements for instances of noncompliance are identified.
 - A procedure for monitoring security requirement compliance by external service providers is established.

Related Resources:

- [View all SP 800-171 System and Services Acquisition Requirements and Assessment Procedures](#)
- [Defense Industrial Base Managed Service Provider Shopping Guide for Small & Medium-Sized Businesses, National Defense ISAC](#)

Getting Started with Supply Chain Risk Management

Family: Supply Chain Risk Management

Description: A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain. [SP 800-53].

Getting Started with Supply Chain Risk Management



Managing supply chain risks is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to identify response actions, and monitoring performance against the plans. Examples of supply chain risks can include: counterfeit or tampered parts, environmental risks (e.g., hurricanes, floods, tornadoes), and technology risks (e.g., cyber incident halting operations of a critical supplier).

Develop a plan— A supply chain risk management plan will look different for every business, as businesses have different supply chains and associated risks. In general, a plan should:

- ✓ Identify critical suppliers that have access to, or provide components to, systems that process, store, or transmit CUI.
- ✓ Define the frequency for reviewing and updating the supply chain risk management plan (e.g., annually, semi-annually)
- ✓ Identify risks associated with the development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. What would the negative impact be if systems are disrupted or compromised?
- ✓ Establish policies for evaluating vendors prior to purchasing components or engaging in services.
- ✓ Identify risk response actions for the identified risks. How will the business respond to a supply chain incident? Are there alternative suppliers or systems to rely upon to keep the business operational during an incident?
- ✓ Define a strategy for monitoring performance against the plan.

Related Resources:

- [View all SP 800-171 Supply Chain Risk Management Requirements and Assessment Procedures](#)
- [NIST Cybersecurity Framework 2.0 Quick Start Guide for Cybersecurity Supply Chain Risk Management](#)
- [Securing Small and Medium-Sized Supply Chains Resource Handbook, CISA](#)
- [Operationalizing Vendor Supply Chain Risk Management Template \(.xlsx\), CISA](#)