



Procurement Technical Assistance Center

**PTAC**

New Mexico

# CYBERSECURITY

**LEARN CONNECT WIN !**

The New Mexico Procurement Technical Assistance Center (NMPTAC) is funded in part through a cooperative agreement with the Defense Logistics Agency.  
The NMPTAC is also funded by the State of New Mexico.

# Overview

- ▶ What We are Protecting
- ▶ Requirements for Protecting Federal Contract Information (FCI)
- ▶ Becoming FCI Cybersecure
- ▶ Protecting Controlled Unclassified Information (CUI)
- ▶ Additional Cyber Requirements for CUI
  - NIST 800-171
  - DFAR 252-204-7012
  - Cybersecurity Maturity Model Certification
- ▶ References

# Definitions

- ▶ **Cybersecurity:** Information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- ▶ **Federal Information System:** An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency
- ▶ **Non-Federal Organization:** An entity that owns, operates, or maintains a nonfederal information system

# What are we protecting ?



# What are We Protecting?

## Public Information

Public Information or information marked for public release.  
Minimum Security Requirements in a non-federal information system: None

## Federal Contract Information (FCI)

Information that is not marked as public or for public release  
Minimum Cybersecurity Requirements in a non-federal information system:  
FAR 52.204-21

## Confidential Business Information

Financial, technical and personal information on company systems

## CUI

Information that is marked or identified as requiring protection under the CUI program.  
Minimum Security Requirements in a non-Federal Information System  
NIST SP 800-171

# Key Concepts

- ▶ FCI is information in your contract or produced by you in the performance of your contract that is not public information.
- ▶ Example: You are asked to provide support for a Base Open House that has yet to be publicly announced.
  - The dates and other event info would be FCI.
  - Your agenda identifying support arrangements timetable etc. are also FCI.
- ▶ FCI can be or can become CUI in which case additional protections beyond FAR 52.204-21 will be required.
- ▶ CUI is unclassified information that is not publicly releasable because a specific regulatory or legal requirement requires its protection.
  - Personally Identifiable Information
  - HIPA
  - Controlled Technical Information
  - Export Controlled
  - Critical Infrastructure
- ▶ CUI Protection described in NIST 800-171
- ▶ DFAR 252-204-12 describes HOW the NIST requirements are applied for DOD
- ▶ The CMMC initiative is a means to independently verify compliance with NIST 800-171

Federal Contract  
Information

Controlled Unclassified  
Information

# Controlled Unclassified Information (CUI)

- ▶ Controlled Unclassified Information (CUI) ...requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
- ▶ The National Archives and Records Administration (NARA) (is designated) as Executive Agent to implement the Order and oversee agency actions to ensure compliance.

# CUI Categories Index Grouping

- ▶ Critical Infrastructure
- ▶ Defense
- ▶ Export Control
- ▶ Financial
- ▶ Immigration
- ▶ Intelligence
- ▶ International Agreements
- ▶ Law Enforcement
- ▶ Legal
- ▶ Natural and Cultural Resources
- ▶ North Atlantic Treaty Organizational (NATO)
- ▶ Nuclear
- ▶ Patent
- ▶ Privacy
- ▶ Procurement and Acquisition
- ▶ Proprietary Business Information
- ▶ Provisional
- ▶ Statistical
- ▶ Tax
- ▶ Transportation



# Example: Controlled Technical Information

- ▶ ... technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- ▶ ... does not include information that is lawfully publicly available without restrictions.
- ▶ ... the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171
- ▶ If the Contractor intends to use an external cloud service provider ... the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline

Description of Data Collected

Requirement to Protect Data

# Regulatory and Contract Requirements for FCI



# Comply with FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

- ▶ Basic Cyber hygiene requirements consistent with business best practices
- ▶ Protects Federal Contract Information (CFI) residing on Covered Contractor Information Systems
- ▶ Achievable by most small businesses with some focused help
- ▶ 15 specific requirements listed in the clause
- ▶ No third-party certification required but can be reviewed during routine audits

# Comply with CUI Requirements if applicable to your contract/customer

- ▶ Requirements for CUI found in National Institute of Standards and Technology Special Publication SP800-171A

# FAR 52.204-21 Requirements

FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	Basic or Derived	800-171 Family
<b>(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</b>	3.1.1	Basic	Access Control
<b>(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.</b>	3.1.2	Basic	Access Control
<b>(iii) Verify and control/limit connections to, and use of,</b>	3.1.20	Derived	Access Control
<b>(iv) Control information posted or processed on publicly accessible information systems.</b>	3.1.22	Derived	Access Control
<b>(v) Identify information system users, processes acting on behalf of users, or devices.</b>	3.5.1	Basic	Identification and Authentication
<b>(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.</b>	3.5.2	Basic	Identification and Authentication

# FAR 52.204-21 Requirements

FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	Basic or Derived	800-171 Family
<b>(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.</b>	3.8.3	Basic	Media Protection
<b>(viii) Limit physical access to organizational Information systems, equipment, and the respective operating environments to authorized individuals.</b>	3.10.1	Basic	Physical Protection
<b>(ix) Escort visitors and monitor visitor activity... ...maintain audit logs of physical access, and... ...control and manage physical access devices.</b>	3.10.3 3.10.4 3.10.5	Derived	Physical Protection
<b>(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.</b>	3.13.1	Basic	System and Communication Protection
<b>(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</b>	3.13.5	Derived	System and Communication Protection
<b>(xii) Identify, report, and correct information and information system flaws in a timely manner.</b>	3.14.1	Basic	System and Information Integrity
<b>(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.</b>	3.14.3	Basic	System and Information Integrity

# FAR 52.204-21 Requirements

FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	Basic or Derived	800-171 Family
<b>(xiv) Update malicious code protection mechanisms when new releases are available.</b>	3.14.4	Derived	System and Information Integrity
<b>(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or</b>	3.14.5	Derived	System and Information Integrity

Other requirements. **This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.**

Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

# Becoming FCI Cybersecure

- »» Achieving compliance with the FAR 52.204-21 Standards



# Cybersecurity is a Risk Management Exercise

## ▶ Risks

- Malicious Code
- Virus
- Worms
- Ransomware
- Physical loss of equipment (theft/fire/etc.)
- Unauthorized Access
- Denial of Service
- Loss of data/confidential information
- Disgruntled employee
- Equipment failure
- Software bugs

## ▶ Responses

- Cybersecurity Practices tailored to each risk

# Items to consider

- ▶ Self- Assessment of devices
- ▶ Policies regarding use of company equipment
- ▶ Cybersecurity Insurance
- ▶ **Computer files backup**
- ▶ Train Employees
  - Employees are your first line of defense
  - They need to feel and understand this
  - Need to know what to look for
  - Who can they go to with questions

# Access Control (AC)

## FAR 52.204-21 b.1.i

- ▶ Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

3.1.1(a)	authorized users are identified.
3.1.1(b)	processes acting on behalf of authorized users are identified.
3.1.1(c)	devices (and other systems) authorized to connect to the system are identified.
3.1.1(d)	system access is limited to authorized users.
3.1.1(e)	system access is limited to processes acting on behalf of authorized users.
3.1.1(f)	system access is limited to authorized devices (including other systems).

# Access Control (AC)

## FAR 52.204-21 b.1.i

- Control who can use company computers and who can log on to the company computers.
- Set up your system so that unauthorized users and devices cannot get on the company network.
- NIST SP 800-171 3.1.1

# Access Control (AC)

## FAR 52.204-21 b.1.ii

- ▶ Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

3.1.2(a)	the types of transactions and functions that authorized users are permitted to execute are defined.
3.1.2(b)	system access is limited to the defined types of transactions and functions for authorized users.

- Make sure to limit users/employees to only the systems, roles, or applications they are permitted to use and that are needed for their job.
- NIST SP 800-171 3.1.2

# Access Control (AC)

## FAR 52.204-21 b.1.iii

- ▶ Verify and control/limit connections to and use of external information systems.

3.1.20(a)	connections to external systems are identified.
3.1.20(b)	the use of external systems is identified.
3.1.20(c)	connections to external systems are verified.
3.1.20(d)	the use of external systems is verified.
3.1.20(e)	connections to external systems are controlled/limited.
3.1.20(f)	the use of external systems is controlled/limited.

# Access Control (AC)

## FAR 52.204-21 b.1.iii

- Make sure to control and manage connections between your company network and outside networks, such as public internet or a network that does not belong to your company.
- Be aware of applications that can be run by outside systems.
- Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information.

# Access Control (AC)

## FAR 52.204-21 b.1.iii (cont.)

- You can also choose to limit how and when your network is connected to outside systems and/or decide that only certain employees can connect to outside systems from network resources.
  
- NIST 800-171-3.1.20



# Access Control (AC)

## FAR 52.204-21 b.1.iv

- ▶ Control information posted or processed on publicly accessible information systems.

3.1.22(a)	individuals authorized to post or process information on publicly accessible systems are identified.
3.1.22(b)	procedures to ensure CUI is not posed or processed on publicly accessible systems area identified.
3.1.22(c)	a review process is in place prior to posting of any content to publicly accessible systems.
3.1.22(d)	content on publicly accessible systems is reviewed to ensure that it does not include CUI.
3.1.22(e)	mechanisms are in place to remove and address improper posting of CUI.

# Access Control (AC)

## FAR 52.204-21 b.1.iv

- Do not allow sensitive information, including FCI, to become public.
- It is important to know which users/employees are allowed to publish information on publicly accessible systems, like your company website.
- Limit and control information that is posted on your company's website(s) that can be accessed by the public.
- NIST SP 800-171 3.1.22

# Identification and Authentication (IDA)

## FAR 52.204-21 b.1.v

- ▶ Identify information system users, processes acting on behalf of users, or devices.

3.5.1(a)	system users are identified.
3.5.1(b)	processes acting on behalf of users are identified.
3.5.1(c)	devices accessing the system are identified.

# Identification and Authentication (IDA) FAR 52.204-21 b.1.v

- Authentication helps you to know who is using or viewing your system.
- Make sure to assign individual, unique identifiers, like user names, to all employees/users who access company systems.
- Confirm the identities of users, process, or devices before allowing them access to the company's information system—usually done through passwords.
- NIST SP 800-171 3.5.1

# Identification and Authentication (IDA)

## FAR 52.204-21 b.1.vi

- ▶ Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

3.5.2(a)	the identity of each user is authenticated or verified as a prerequisite to system access.
3.5.2(b)	the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.
3.5.2(c)	the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

# Identification and Authentication (IDA)

## FAR 52.204–21 b.1.vi

- Before you let a person or a device have access to your system, you need to verify that user or device is who or what it claims to be.
- This verification is called authentication.
- The most common way to verify identity is using a username and a hard-to-guess password.
- NIST SP 800–171 3.5.2

# Media Protection (MP)

## FAR 52.204-21 b.1.vii

- ▶ Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

3.8.3(a)	system media containing CUI is sanitized or destroyed before disposal.
3.8.3(b)	system media containing CUI is sanitized before is released for reuse.

- In this case, “media” can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones.

# Media Protection (MP)

## FAR 52.204-21 b.1.vii (cont.)

- It is important to see what information is on these types of media.
- If there is Federal contract information (FCI) – information you or your company got doing work for the Federal government that is not shared publicly–you or someone in your company should do one of two things before throwing the media away:
  - Clean or purge the information, if you want to reuse the device, or
  - Shred or destroy the device so it cannot be read.

NIST SP 800-171 3.8.3



# Physical Protection (PP)

## FAR 52.204-21 b.1.viii

- ▶ Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

3.10.1(a)	authorized individuals allowed physical access are identified.
3.10.1(b)	physical access to organizational systems is limited to authorized individuals.
3.10.1(c)	physical access to equipment is limited to authorized individuals.
3.10.1(d)	physical access to operating environments is limited to authorized individuals.

# Physical Protection (PP)

## FAR 52.204-21 b.1 .viii

- Think about what parts of your physical space (office, plant, factory, etc.) what equipment, including the network, need to be protected from physical contact.
- For those parts of your company where you want only specific employees to have physical access to, monitor or limit who is able to enter those spaces with badges, key cards, etc.
- NIST SP 800-171 3.10.1

# Physical Protection (PP)

## FAR 52.204-21 Partial b.1.ix

### ▶ Escort visitors and monitor visitor activity.

3.10.3(a)	visitors are escorted.
3.10.3(b)	visitor activity is monitored.

- Do not allow visitors, even those people you know well, to walk around your facility without an escort.
- Make sure that all non-employees wear special visitor badges and/or are escorted by an employee at all times while on your property.
- NIST SP 800-171 3.10.3

# Physical Protection (PP)

## FAR 52.204-21 Partial b.1.ix

### ▶ Maintain audit logs of physical access.

Determine if audit logs of physical access are maintained.

- Make sure you have a record of who is accessing both your facility (office, plant, factory, etc.) and your equipment.
- You can do this in writing by having employees and visitors sign in and sign out as they enter and leave your physical space, and be keeping a record of who is coming and going from the facility.
- NIST SP 800-171 3.10.4

# Physical Protection (PP)

## FAR 52.204-21 Partial b.1.ix

- ▶ Control and manage physical access devices.

3.10.5(a)	physical access devices are identified.
3.10.5(b)	physical access devices are controlled.
3.10.5(c)	physical access devices are managed.

# Physical Protection (PP)

## FAR 52.204-21 Partial b.1.ix

- Controlling physical access devices like locks, badging, key cards, etc. Is just as important as monitoring and limiting who is able to physically access certain equipment.
- Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.
- NIST SP 800-171 3.10.5

# System and Communication Protection (SCP) FAR 52.204-21 b.1.x

- ▶ Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

3.13.1(a)	the external system boundary is defined.
3.13.1(b)	key internal system boundaries are defined.
3.13.1(c)	communications are monitored at the external system boundary.
3.13.1(d)	communications are monitored at key internal boundaries
3.13.1(e)	communications are controlled at the external system boundary.
3.13.1(f)	communications are controlled at key internal boundaries.
3.13.1(g)	communications are protected at the external system boundary.
3.13.1(h)	communications are protected at key internal boundaries.

# System and Communication Protection (SCP) FAR 52.204–21 b.1.x

- Just as your office or plant has fences and locks for protection from the outside, and uses badges and keycards to keep non-employees out, your company's IT network or system has boundaries that must be protected.
- Most companies use a web proxy and a firewall.
  - Enforcement is accomplished automatically by system policies enforced by the firewall.
- NIST SP 800–171 3.13.1



# System and Communication Protection (SCP) FAR 52.204-21 b.1.xi

- ▶ Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

3.13.5(a)	publicly accessible system components are identified.
3.13.5(b)	subnetworks for publicly accessible system components are physically or logically separated from internal networks.

# System and Communication Protection (SCP) FAR 52.204-21 b.1.xi

- Separate the publicly accessible systems from the internal systems that need to be protected.
  - Especially important in Home Office situations
  - Easily implemented with firewall
- Do not place the internal systems on the same network as the publicly accessible systems.
- NIST SP 800-171 3.13.5

# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xii

- ▶ Identify, report, and correct information and information system flaws in a timely manner.

3.14.1(a)	the time within which to identify system flaws is specified.
3.14.1(b)	system flaws are identified within the specified time frame.
3.14.1(c)	the time within which to report system flaws is specified.
3.14.1(d)	system flaws are reported within the specified time frame.
3.14.1(e)	the time within which to correct system flaws is specified.
3.14.1(f)	system flaws are corrected within the specified time frame.

# System and Informational Integrity (SII)

## FAR 52.204–21 b.1.xii

- Be aware of problems in the software and computer equipment your company uses.
- Consider purchasing support from your hardware and software vendors/suppliers, getting patches, and signing up for IT newsletters with updates about common problems or weaknesses in software.
- Install security updates promptly.
  - Enable auto updates
- NIST SP 800–171 3.14.1

# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xiii

- ▶ Provide protection from malicious code at appropriate locations within organizational information systems.

3.14.2(a)	designated locations for malicious code protection are identified.
3.14.2(b)	protection from malicious code at designated locations is provided.

# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xiii

- You can protect your company's valuable IT system by stopping malicious code at designated locations in your system.
  - Sandboxing at the firewall
  - Anti-malware at system endpoints
    - Computer
    - Cell phones
- Malicious code is program code that purposefully creates an unauthorized function or process that will have a negative impact on the confidentiality, integrity, or availability of an information system.
- NIST SP 800-171 3.14.2

# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xiv

- ▶ Update malicious code protection mechanisms when new releases are available.
- ▶ Determine if malicious code protection mechanisms are updated when new releases are available.

# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xiv

- You can protect your company's valuable IT systems by staying up to date on new security releases that stop malicious code and monitoring the system regularly.
  - Malware/endpoint protection updates automatically downloaded and installed.
  - Keep abreast of newly emerging threats through periodic updates.
- NIST SP 800-171 3.14.4



# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xv

- ▶ Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.5(a)	the frequency for malicious code scans is defined.
3.14.5(b)	malicious code scans are performed with the defined frequency.
3.14.5( c)	real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

# System and Informational Integrity (SII)

## FAR 52.204-21 b.1.xv

- Companies should use anti-malware software to scan and identify viruses in their computer systems and have a plan for how often scans are conducted.
  - Real-time scans will look at the system whenever new files are downloaded, opened, and saved.
  - Periodic scans check previously saved files against updated malware information.
- NIST SP 800-171-3.14.5

# Protecting CUI

»» Procedural Guidance

# Who is your Government Customer? Does it Matter?



# Protection

- ▶ CUI must be protected against unauthorized disclosure loss or theft.
- ▶ The protections afforded its protection are driven by risk (likelihood and impact)
- ▶ Procedures are driven by media – electronic or physical
- ▶ Procedures also differ between DoD/Homeland Security and other Federal Agencies
  - DFARS 252.204–7012 (DoD)
  - Unspecified implementation of NIST 800–171

# Protecting Controlled Unclassified Information

- ▶ The principal force behind the government's contractor cybersecurity requirements is protecting against the loss of critical intellectual property and sensitive information.
- ▶ Billions of dollars worth of Research and Development data has been stolen by various individuals or nation states allowing them to leap ahead of the US without significant costs
- ▶ Critical defense or privacy information is being stolen and sold

# Protecting CUI

- ▶ Refer to Online Repository  
(<https://www.archives.gov/cui/registry/categorylist>)
- ▶ Identifies approved CUI categories
- ▶ Includes marking, handling, and storage procedures for CUI items

# CUI Category: Controlled Technical Information

## Banner Marking: CUI//SP-CTI

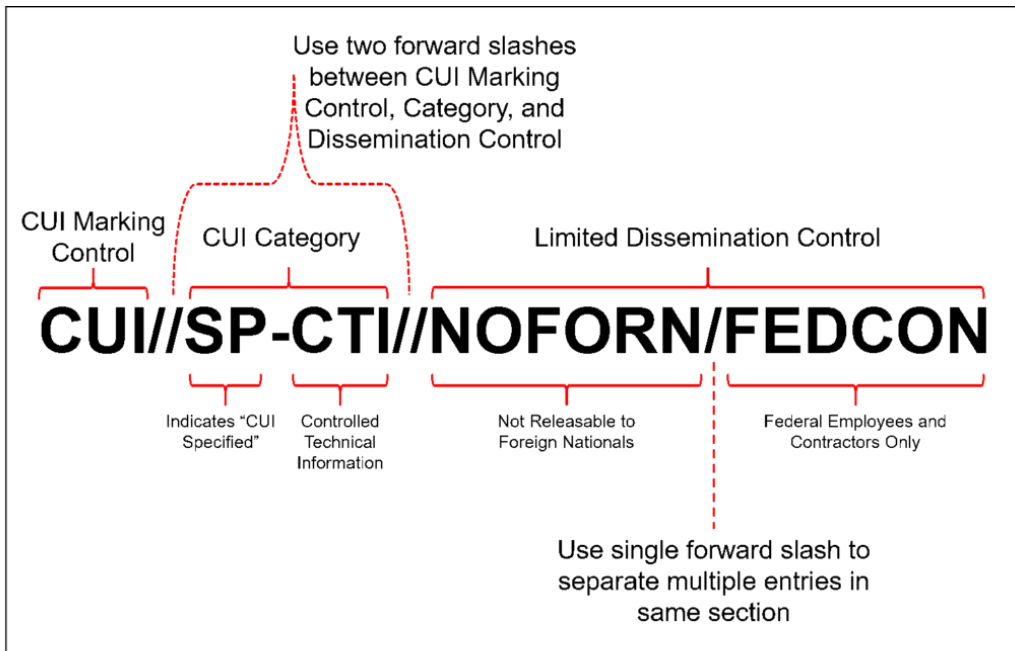
<p><b>Category Description:</b></p>	<p>Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, 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.</p>
<p><b>Category Marking:</b></p>	<p>CTI</p>
<p><b>Banner Format and Marking Notes:</b></p>	<p>Banner Format: CUI//Category Marking//Limited Dissemination Control</p> <p>Marking Notes:</p> <ul style="list-style-type: none"> <li>• The CUI Control Marking may consist of either the word "CONTROLLED" or the acronym "CUI", depending on agency policy.</li> <li>• Category marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control.</li> <li>• Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control</li> <li>• Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI.</li> <li>• Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control</li> <li>• Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control</li> <li>• Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control</li> <li>• Reference <a href="#">32 CFR 2002.20</a>, <a href="#">CUI Marking Handbook</a>, <a href="#">Limited Dissemination Controls</a> and individual agency policy for additional and specific marking guidelines</li> </ul>



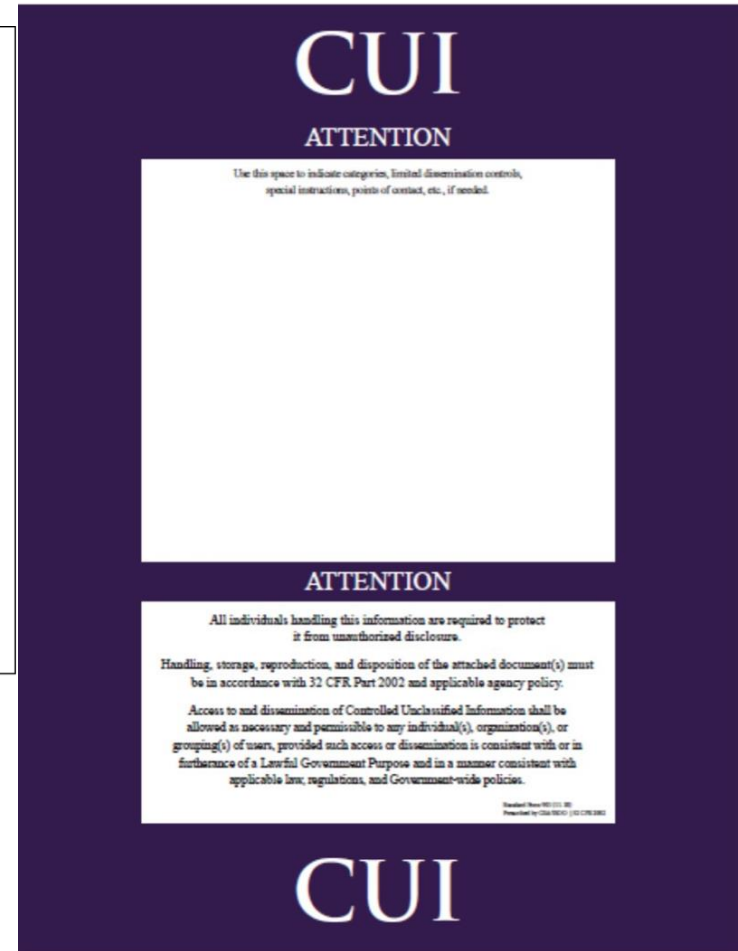
# Storage and Handling of CUI

- ▶ Physical Media (e.g., paper copies, disks, etc.)
  - Must be marked appropriately
  - Must be stored in locked container or cabinet when not in use
  - Cover sheets to protect inadvertent disclosure

# CUI Markings



Banner marking with CUI Specified and multiple limited dissemination controls



# Storage and Handling of CUI

- ▶ Electronic Data
  - Electronic data must be afforded “Adequate Protection” through appropriate cybersecurity measures

# What Security Measures are “Adequate”

- ▶ **No Systems are completely secure.**
- ▶ **But can we really define “adequate retrospectively?”**
  - Your security was not adequate if you did not employ industry and sector appropriate measures.
  - Your security was not adequate if you did not have a plan to secure your systems
  - Your security was not adequate if you did not perform a risk assessment.
- ▶ **If you did all these and still were breached, then the answer is less clear.**
- ▶ **NIST SP 800–171 describes good practices that must be followed. If they are not followed, then your security measures are definitely not “Adequate”.**

# Securing the Supply Chain

- ▶ The Cybersecurity requirements do not simply apply to the prime contractor
- ▶ Cybersecurity is a mandatory flow-down requirement to lower tier contractors and subcontractors at all levels
- ▶ This is even true of the Basic FAR: FAR 52.204-21 requirements in Commercial Contracts!
- ▶ The intent is to secure the entire supply chain at all levels.

# Prime Contractor Responsibilities

- ▶ Fundamental requirement to manage subcontractors (see Far 42.202(e)(2))
- ▶ Remember, the only actual parties to a Government contract are the Government and the prime contractor
- ▶ Understand what constitutes CDI under the clause
  - ▶ – CDI includes unclassified CTI or other information contained in NARAs CUI Registry
- ▶ Maintain an open, written dialogue with the CO to determine the type of data at play
- ▶ Ensure that the clause is appropriately included in subcontracts

# Prime Contract Responsibilities (Cont.)

- ▶ Conduct proper due diligence on all proposed subcontractors
- ▶ Understand the consequences of noncompliance
  - – Breach
  - – Termination
  - – Past Performance Issues
  - – Potential FCA allegations

# Do not Comply

- ▶ Contractors who do not comply with these requirements are subject to Termination for Default.
- ▶ 31 U.S. Code § 3729. False claims
  - Knowingly present or cause to be presented to the United States a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A));
  - Knowingly make, use, or cause to be made or used a false record or statement to get a false or fraudulent claim paid or approved (31 U.S.C. § 3729(a)(1)(B))



# Regulatory & Contract Requirements for Protecting Controlled Unclassified Information (CUI)

- » Unique requirements for Cybersecurity when CUI is present

# National Institute of Standards and Technology (NIST)

- ▶ Government-wide applicability of standards and guidelines
- ▶ Cybersecurity focal point
  - NIST Special Publications 800 series provide all agency guidance
  - NIST 800-171 series focused on protection of CUI
- ▶ Cybersecurity Framework establishes the ‘best practices’ approach to implementing their recommendations

# NIST Cybersecurity Framework

- ▶ The NIST Cybersecurity Framework, created thru collaboration between govt. & private sector, uses common Language to address and manage cybersecurity risk in cost-effective way based on business needs

- ▶ FRAMEWORK CORE:

- Identifies
- Protect
- Detect
- Respond
- Recover



# Cybersecurity Framework

- ▶ Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- ▶ Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

# Cybersecurity Framework

- ▶ Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- ▶ Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
- ▶ Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

# Security Requirements

▶ <b>NIST 800–171 Security Families</b>	
▶ AC – Access Control (3.1)	22
▶ AT – Awareness & Training (3.2)	3
▶ AU – Audit & Accountability (3.3)	9
▶ CM – Configuration Management (3.4)	9
▶ IA – Identification & Authentication (3.5)	11
▶ IR – Incident Response (3.6)	3
▶ MA – Maintenance (3.7)	6
▶ MP – Media Protection (3.8)	9
▶ PS – Personnel Security (3.9)	2
▶ PE – Physical Protection (3.10)	6
▶ RA – Risk Assessment (3.11)	3
▶ CA – Security Assessment (3.12)	4
▶ SC – System & Communications Protection (3.13)	16
▶ SI – System & Information Integrity (3.14)	7
▶ TOTAL REQUIREMENTS:	<u>110</u>

# NIST/FAR Requirements

NIST 800-171 Security Families	R1	Objectives	A	FAR
AC – Access Control (3.1)	22	48	70	4
AT – Awareness & Training (3.2)	3	6	9	
AU – Audit & Accountability (3.3)	9	20	29	
CM – Configuration Management (3.4)	9	35	44	
IA – Identification & Authentication (3.5)	11	14	25	2
IR – Incident Response (3.6)	3	11	14	
MA – Maintenance (3.7)	6	4	10	
MP – Media Protection (3.8)	9	6	15	1
PS – Personnel Security (3.9)	2	2	4	
PE – Physical Protection (3.10)	6	10	16	4
RA – Risk Assessment (3.11)	3	6	9	
CA – Security Assessment (3.12)	4	10	14	
SC – System & Communications Protection (3.13)	16	25	41	2
SI – System & Information Integrity (3.14)	7	13	20	4
<b>TOTAL REQUIREMENTS:</b>	<b>110</b>	<b>210</b>	<b>320</b>	<b>17</b>

# 3-Step Process to Complying with Cybersecurity Requirements



- ▶ **STEP 1: Develop System Security Plan (SSP) describing**
  - The system boundary;
  - The operational environment;
  - How the security requirements are implemented; and
  - The relationships with or connections to other systems
- ▶ **STEP 2: Conduct Assessment, Produce Security Assessment Report**
  - Conducted against security requirements in NIST SP 800-171
- ▶ **STEP 3: Produce a Plan of Action with Milestones (POAM)**
  - Should describe how any unimplemented security requirements will be met and how any planned improvements will be implemented
  - Should include detailed milestones used to measure progress



# Department of Defense Implementation of NIST 800-171

- ▶ FAR 52.204-21 (FCI) in nearly every contract
- ▶ DFARS Clauses tailored to Protect CUI
  - 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls (Provision)
  - 252.204.7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Clause)
  - 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements (Provision)
  - 252.204-7020 NIST SP 800-171 DoD Assessment Requirements (Clause)
  - 252.204-7021 Cybersecurity Maturity Model Certification Requirements (Clause)

# Cyber Security Compliance Requirements

## FAR 52.204-21

- **Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)**
- 2014 and 2016 Implementation
- No Grace Period for Compliance
- 15 Controls
- Considered Minimum Compliance Criteria
- Federal Contract Information (FCI)

## DFARS 252.204-7012

- **Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)**
- Compliance or POAM required:
  - 30 Days from Award
  - SSP + POAM is Compliant even if all 110 Controls not met
- 110 Controls
- Oct 2016 Update added SSP + POAM Control to allow for Phase-in Period
- Covered Defense Information (CDI)

## NIST SP 800-171

- **Special Publication: Protecting Unclassified Information in Nonfederal Information Systems and Organizations**
- Sets Industry Standard Practice
- 110 Controls
  - Physical Site Controls
  - Computer System Controls
  - Process Security Controls

# Cyber Security Compliance Requirements

## DFARS 252.204-7019

- Notice of NIST SP 800-171 DoD Assessment Requirements. BASIC (Nov 2020)
- Requires offerors to upload a self assessment in SPRS prior to receiving a DoD award.
- Effective December 1, 2020.

## DFARS 252.204-7020

- NIST SP DoD Assessment Requirements (Nov 2020)
- Requires a contractor to provide the Government access to its facilities, systems, and personnel to conduct or renew a higher-level assessment.

## DFARS 252.204-7021

- DoD Assessment and CMMC assessments (Nov 2020)
- The contractor is to maintain the requisite CMMC level for the duration of the contract.

# DFARS Interim Rule

- ▶ DFARS 252.204-2019
  - Effective December 1, 2020
  - Required to implement NIST SP 800-171
  - Post assessment in Supplier Performance Risk System (SPRS)
    - <https://www.sprs.csd.disa.mil/>
  - Prior to receiving an award
  - Prior to any Option year award
  
- ▶ Comment period ended 11/30/2020
  - <https://beta.regulations.gov/document/DARS-2020-0034-0001>

# SPRS Registration

- ▶ To register on SPRS you will need a Procurement Integrated Enterprise Environment (PIEE) login
  - <https://piee.eb.mil/piee-landing/>
- ▶ You will need a cage code
- ▶ Then you will need to call PIEE helpdesk (1-866-618-5988) to register your cage code

# PIEE Registration

- ▶ Once you receive confirmation of cage code registration log on to PIEE system:
  - <https://piee.eb.mil/piee-landing/>
- ▶ Once in the system need to identify a Contract Administration Manager (CAM)
  - Gate Keeper
- ▶ Click "Register" (found in the upper right-hand corner of the screen) • Click "Agree"
- ▶ • Select the user type "Vendor"
- ▶ • Select "User ID \ Password" from the drop down menu • Create a personal User ID and Password with the criteria presented on the screen and click "Next"
- ▶ • Fill out the "User Profile" section and click "Next"
- ▶ • Fill out the "Company Information" section of the page (the "Supervisor Information" section can be left blank) and click "Next"

# PIEE Registration Steps

- ▶ • Fill out the "Security Questions" (Three different questions with three different answers are required) and click "Next"
- ▶ • Select the PIEE Application
- ▶ • Select the Contractor Administrator Role • Click "Add Roles"
- ▶ • Click "Group Lookup"
- ▶ • Enter your CAGE code and hit click "Search" then "Search by Location Code" Select your CAGE code Group (ie. TOP\OGDEN VENDORS\your cage code") • Click "Next"
- ▶ • Enter the reason you are requesting the Contractor Administrator Role in the "Justification" field and click "Next"
- ▶ • Click "Next"
- ▶ • Verify all your entries are correct and click "Next"
- ▶ • Read and accept the statement of accountability • Click on the signature block and re-enter your password.
- ▶ • Click "Submit Registration"
- ▶ • These steps should complete the registration.
- ▶ **Help Desk 1-866-618-5988**

# SPRS Cybersecurity Score

- ▶ Required by DFARS 252.204-7020 – NIST SP 800-171 DoD Assessment Requirements
  - Score is self-reported based on NIST 800-171A Self Assessment of the 110 requirements
  - Interim measure pending CMMC implementation over next 5 years
- ▶ Three Levels of Confidence concerning score:
  - Basic – accept contractor’s self assessment at face value
  - Medium – Government personnel perform a desktop review of self assessment to improve confidence
  - High – Government personnel perform a in-person review of assessment including contractor demonstrations of compliance.



# NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020

## *NIST SP 800-171 DoD Assessment Scoring Template*

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

# SPRS Score

- ▶ Using the CMMC as a guide to the levels following are the scores to use as a guide.
- ▶ Level 1(Basic)
  - $110 - 250 = <140>$  (Should be the lowest score)
- ▶ Level 2(Medium)
  - $110 - 109 = 1$
- ▶ Level 3(High)
  - $110 - 0 = 110$

# Perform a Self-Assessment

- ▶ Use NIST Handbook 162 to perform a Self-Assessment of your company.
  - Not everything in this handbook will apply to every business situation.

<https://csrc.nist.gov/publications/detail/sp/800-162/final>

**NIST Handbook 162**

**NIST MEP Cybersecurity  
Self-Assessment Handbook  
For Assessing NIST SP 800-171  
Security Requirements in Response to  
DFARS Cybersecurity Requirements**

Patricia Toth

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.HB.162>

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# Cybersecurity Maturity Model Certification (CMMC)

- ▶ Goal is to transition from the Self-assessment and Basic, Medium, High evaluation to CMMC within next five years
- ▶ CMMC adds Independent e.g., third-party assessment of cybersecurity compliance
- ▶ Based on same NIST 800-171A requirements
- ▶ Initial and periodic reassessment

# CMMC

- ▶ DFARS 252.204-7021 – Cybersecurity Maturity Model Certification (CMMC)
  - Desired end state for DOD Cybersecurity
  - The CMMC model measures cybersecurity maturity with five levels and aligns asset of processes and practices with the type and sensitivity of information to be protected and the associated range of threats.
  - The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community.

# CMMC Levels

- ▶ Level 1: Safeguard Federal Contract Information (FCI)
- ▶ Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- ▶ Level 3: Protect Controlled Unclassified Information (CUI)
- ▶ Level 4–5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

# CMMC

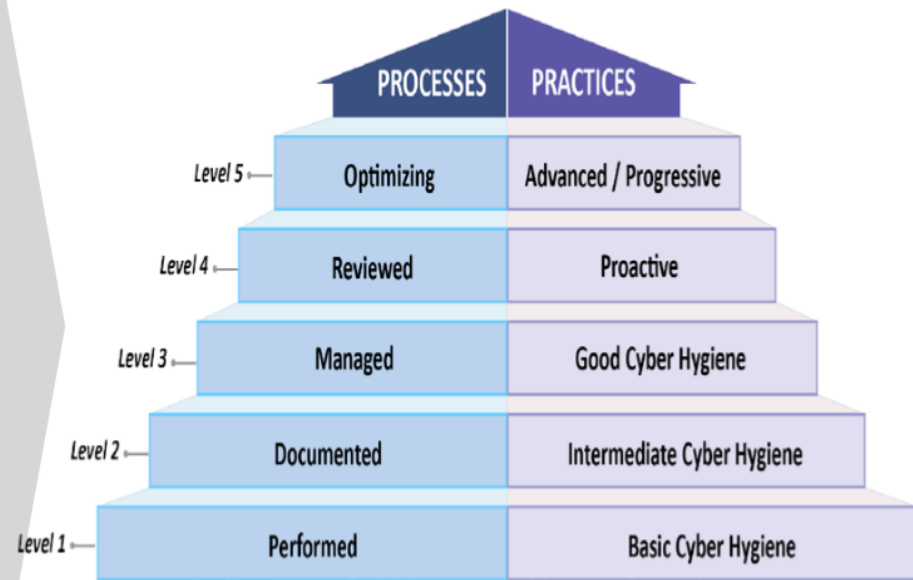
- ▶ Cybersecurity Maturity Model Certification (CMMC)
  - The CMMC model measures cybersecurity maturity with five levels and aligns asset of processes and practices with the type and sensitivity of information to be protected and the associated range of threats.
  - The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community.

# CMMC Model Structure

17 Capability Domains (v1.0)

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

CMMC Model with 5 levels measures cybersecurity maturity





# Focus

- ▶ Level 1: Safeguard Federal Contract Information (FCI)
- ▶ Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- ▶ Level 3: Protect Controlled Unclassified Information (CUI)
- ▶ Level 4–5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

# CMMC Level 1

- ▶ **Processes: Performed**
  - Level 1 requires that an organization performs the specified practices. Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation, process maturity is not assessed for Level 1
- ▶ **Practices: Basic Cyber Hygiene**
  - Level 1 focuses on the protection of FCI and consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 (“Basic Safeguarding of Covered Contractor Information Systems”).

# CMMC Level 2

- ▶ **Processes: Documented**
  - Level 2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented.

# CMMC Level 2 (cont.)

- ▶ Practices: Intermediate Cyber Hygiene
  - Level 2 serves as a progression from Level 1 to 3 and consist of a subset of security requirements specified in NIST SP 800–171 as well as practices from other standards and references. Because this level represents a transitional stage, a subset of the practices reference the protection of CUI.

# CMMC Level 3

- ▶ **Processes: Managed**
  - Level 3 requires that an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders.

# CMMC Level 3 (cont.)

- ▶ Practices: Good Cyber Hygiene
  - Level 3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800–171 as well as additional practices from other standards and references to mitigate threats.
  - It is noted that DFARS clause 252.204–7012 (“Safeguarding of Covered Defense Information and Cyber Incident Reporting”) specifies additional requirements beyond the NIST SP 800–171 security requirements such as incident reporting.

# CMMC Level 4

## ▶ Process: Reviewed

- Level 4 requires that an organization review and measure practices for effectiveness. In addition to measuring practices for effectiveness, organizations at this level are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis.

# CMMC Level 4 (cont.)

- ▶ Practices: Proactive
- ▶ Level 4 focuses on the protection of CUI from APTs and encompasses a subset of the enhanced security requirements from Draft NIST SP 800-171B as well as other cybersecurity best practices. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques, and procedures (TTPs) used by APTs.



# CMMC Level 5

- ▶ **Processes: Optimizing**
  - Level 5 requires an organization to standardize and optimize process implementation across the organization.
- ▶ **Practices: Advanced/Proactive**
  - Level 5 focuses on the protection of CUI from APTs. The additional practices increase the depth and sophistication of cybersecurity capabilities.

# CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

## DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C001 Establish system access requirements	<p>P1001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</p> <ul style="list-style-type: none"> <li>• FAR Clause 52.204-21 b.1.i</li> <li>• NIST SP 800-171 3.1.1</li> <li>• AU ACSC Essential Eight</li> </ul>	<p>P1005 Provide privacy and security notices consistent with applicable Federal Contract Information rules.</p> <ul style="list-style-type: none"> <li>• NIST SP 800-171 3.1.9</li> </ul>	
		<p>P1006 Limit use of portable storage devices on external systems.</p> <ul style="list-style-type: none"> <li>• NIST SP 800-171 3.1.21</li> </ul>	
C002 Control internal system access	<p>P1002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.</p> <ul style="list-style-type: none"> <li>• FAR Clause 52.204-21 b.1.ii</li> <li>• NIST SP 800-171 3.1.2</li> </ul>	<p>P1007 Employ the principle of least privilege, including for specific security functions and privileged accounts.</p> <ul style="list-style-type: none"> <li>• NIST SP 800-171 3.1.5</li> <li>• UK NCSC Cyber Essentials</li> </ul>	<p>P1017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.</p> <ul style="list-style-type: none"> <li>• NIST SP 800-171 3.1.4</li> </ul>

# CMMC Certification

- ▶ CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors that have been accredited by the CMMC AB will perform CMMC assessments
- ▶ CMMC assessment will not be made public.
- ▶ The only information that will be publically available is that your company has a CMMC certification.
- ▶ The specific certification level will NOT be made public.
- ▶ The DoD, however, will have access to all DIB companies' certification levels.

# Summary

- ▶ FAR Clause 52.204-21 should be in place already
- ▶ NIST Special Publication 800-171 defines security requirements for CUI
- ▶ Federal Acquisition Regulation (FAR) are currently being updated to include SP800-171
- ▶ SP 800-171 has been incorporated into DFARS clause 252.204-7012

# Comply with CUI Requirements if applicable to your contract/customer

- ▶ Requirements found in National Institute of Standards and Technology Special Publication SP800-171A
- ▶ Total of 110 individual requirements
- ▶ Perform Self-assessment of current state of compliance
- ▶ Report score to SPRS (DFARS)
- ▶ Continue to address shortfalls and update score

# Links of Resources Available

# Resources Available

- ▶ FAR Clause 52.204-21
  - <https://www.acquisition.gov/content/regulations>
- ▶ NIST SP 800-171
  - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>
- ▶ CUI Registry
  - <https://www.archives.gov/cui/registry/category-list>
- ▶ DFARS 252.204-7012
  - <https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>

# Resources Available

- ▶ Cybersecurity Self-Assessment Handbook (NIST Handbook 162)
  - <https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>
- ▶ Cybersecurity Template
  - <https://gtpac.org/cybersecurity-training-video/>
- ▶ U.S. Department of Energy (DOE O 205.1 C)
  - <https://www.directives.doe.gov/directives-documents/200-series/0205.1-BOrder-c/@@images/file>



# Resources Available

- ▶ System Administration, Networking, and Security (SANS)
  - <https://www.sans.org/account/loginsso>
- ▶ Stay Safe Online
  - <https://staysafeonline.org/>
- ▶ Department of Homeland Security
  - <https://www.us-cert.gov/resources/assessments>
- ▶ Federal Trade Commission
  - <https://www.ftc.gov/tips-advice/business-center/small-businesses>

# Resources Available

- ▶ Steady Networks
  - ▶ [www.steadynetworks.com](http://www.steadynetworks.com)
  - ▶ *Phone: (505) 365-1975*
  
- ▶ *Cova Strategies, LLC*
  - ▶ [cmmc@covastrategies.com](mailto:cmmc@covastrategies.com)
  - ▶ *Phone: (505) 933-9184*
  
- ▶ Tillman Cyber Services, LLC
  - [chad@tillmancyber.com](mailto:chad@tillmancyber.com)
  - Office: (505) 688-4726
  - [www.tillmancyber.com](http://www.tillmancyber.com)

# Resources Available

- ▶ Totem Tech
  - [christian@totem.tech](mailto:christian@totem.tech)
  - Office: (855) 405-4075
  - <https://www.totem.tech/>
- ▶ Left Brain Professionals
  - [Support@LeftBrainPro.com](mailto:Support@LeftBrainPro.com)
  - Office: (614) 556-4415
  - <https://www.leftbrainpro.com/our-team/>
- ▶ Core Business Solutions, Inc
  - [info@thecoresolution.com](mailto:info@thecoresolution.com)
  - Office: 866.354.0300
  - [www.thecoresolution.com](http://www.thecoresolution.com)

# Resources Available

- ▶ NCMA Rio Grande Chapter
  - <https://ncmargc.org/>
- ▶ NM Technology
  - <https://nmtechcouncil.org/about-nmtc/>
- ▶ Manufacturing Extension Partnership (MEP)
  - <https://nmtechcouncil.org/about-nmtc/>
- ▶ Project Spectrum
  - <https://projectspectrum.io/#!/>
  - Project Spectrum is an initiative supported by the Department of Defense [Office of Small Business Programs](#).

# CMMC Resources

- ▶ Cybersecurity Maturity Model Certification
  - <https://www.acq.osd.mil/cmmc/index.html>
- ▶ CMMC Accreditation Body
  - <https://www.cmmcab.org/>
- ▶ CMMC Audit Preparation
  - <https://www.cmmcaudit.org/how-to-become-a-cmmc-auditor-or-certifier/>
- ▶ Securing the DoD Supply Chain
  - <https://www.youtube.com/watch?v=1tnaeEU6Az8&feature=youtu.be>

# References

- ▶ NIST Presentation 10/18/2017
  - David Stieren, Division Chief, Programs and Partnerships
- ▶ Georgia Institute of Technology
  - The Georgia Institute of Technology, commonly referred to as Georgia Tech, is a public research university in Atlanta, Georgia, in the United States.
- ▶ Webinars
  - Cyber Collaboration Center
  - eResilience
  - NICE (National Initiative for Cybersecurity Education)
  - USC University of Southern California

# Thank you for joining us today

For More Information Contact:

**Elythia McAnarney, CPCM, CFCM**  
**PTAC Advisor**

**Elythia.mcanarney@sfcc.edu**

**505-224-5964**

**[www.nmptac.org](http://www.nmptac.org)**

NIST Special Publication 800-171A

---

# Assessing Security Requirements for Controlled Unclassified Information

---

RON ROSS  
KELLEY DEMPSEY  
VICTORIA PILLITTERI

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



NIST Special Publication 800-171A

# Assessing Security Requirements for Controlled Unclassified Information

RON ROSS  
KELLEY DEMPSEY  
VICTORIA PILLITTERI  
*Computer Security Division  
National Institute of Standards and Technology*

June 2018



U.S. Department of Commerce  
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology  
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

## Authority

This publication has been developed by the National Institute of Standards and Technology to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-171A  
Natl. Inst. Stand. Technol. Spec. Publ. 800-171A, **92 pages** (June 2018)

CODEN: NSPUE2

This publication is available free of charge from:

<https://doi.org/10.6028/NIST.SP.800-171A>

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

### Comments on this publication may be submitted to:

National Institute of Standards and Technology  
Attn: Computer Security Division, Information Technology Laboratory  
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930  
Email: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)

All comments are subject to release under the Freedom of Information Act (FOIA).

## Reports on Computer Systems Technology

The NIST Information Technology Laboratory (ITL) promotes the United States economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related information and protection of individuals' privacy in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and its collaborative activities with industry, government, and academic organizations.

### Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. This publication provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in [NIST Special Publication 800-171](#), *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments. Security assessments can be conducted as self-assessments; independent, third-party assessments; or government-sponsored assessments and can be applied with various degrees of rigor, based on customer-defined depth and coverage attributes. The findings and evidence produced during the security assessments can facilitate risk-based decisions by organizations related to the CUI requirements.

### Keywords

Assessment; Assessment Method; Assessment Object; Assessment Procedure; Assurance; Basic Security Requirement; Controlled Unclassified Information; Coverage; CUI Registry; Depth; Derived Security Requirement; Executive Order 13556; FISMA; NIST Special Publication 800-53; NIST Special Publication 800-53A; Nonfederal Organization; Nonfederal System; Security Assessment; Security Control.

## Acknowledgements

The authors gratefully acknowledge and appreciate the contributions from Jon Boyens, Devin Casey, Chris Enloe, Ned Goren, Gary Guissanie, Jody Jacobs, Jeff Marron, Vicki Michetti, Mark Riddle, Mary Thomas, Matt Scholl, Gary Stoneburner, Patricia Toth, and Patrick Viscuso whose thoughtful and constructive comments improved the quality, thoroughness, and usefulness of this publication. A special note of thanks goes to Jim Foti and Elizabeth Lennon for their superb administrative and technical editing support.

### CAUTIONARY NOTE

The generalized assessment procedures described in this publication provide a framework and a starting point for developing specific procedures to assess the CUI security requirements in [NIST Special Publication 800-171](#). The assessment procedures can be used to generate relevant evidence to determine if the security safeguards employed by organizations are implemented correctly, are operating as intended, and satisfy the CUI security requirements. Organizations have the flexibility to specialize the assessment procedures by selecting the specific assessment methods and the set of assessment objects to achieve the assessment objectives. There is no expectation that all assessment methods and all objects will be used for every assessment. There is also significant flexibility on the scope of the assessment and the degree of rigor applied during the assessment process. The assessment procedures and methods can be applied across a continuum of approaches—including self-assessments; independent, third-party assessments; and assessments conducted by sponsoring organizations (e.g., government agencies). Such approaches may be specified in contracts or in agreements by participating parties.

### DEFINITION AND USAGE OF THE TERM INFORMATION SYSTEM

Unless otherwise specified by legislation, regulation, or governmentwide policy, the use of the term *information system* in this publication is replaced by the term *system*. This change reflects a more broad-based and holistic definition of information systems that includes, for example: general purpose information systems; industrial and process control systems; cyber-physical systems; and individual devices that are part of the Internet of Things. As computing platforms and information technologies are increasingly deployed ubiquitously worldwide and systems and components are connected through wired and wireless networks, the susceptibility of Controlled Unclassified Information to loss or compromise grows—as does the potential for adverse consequences resulting from such occurrences.

### OTHER RESOURCES TO SUPPORT ASSESSMENTS

NIST Special Publication 800-171A is a companion publication developed to support assessments of the CUI security requirements in [NIST Special Publication 800-171](#). As such, it is the primary and authoritative source of guidance for organizations conducting such assessments. However, since it is recognized that the communities of interest affected by the CUI security requirements are broad and diverse, other supporting assessment guidance may be developed for those communities. For example, the NIST Manufacturing Extension Partnership (MEP) developed [Handbook 162, NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements](#). This resource, along with other assessment resources that may be developed in the future, can complement the assessment procedures in NIST Special Publication 800-171A, thus helping sector-specific organizations generate the evidence needed to determine if the CUI security requirements have been satisfied.

## Table of Contents

<b>CHAPTER ONE</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	PURPOSE AND APPLICABILITY	1
1.2	TARGET AUDIENCE	2
1.3	ORGANIZATION OF THIS SPECIAL PUBLICATION	2
<b>CHAPTER TWO</b>	<b>THE FUNDAMENTALS</b>	<b>4</b>
2.1	ASSESSMENT PROCEDURES	4
2.2	ASSURANCE CASES	6
<b>CHAPTER THREE</b>	<b>THE PROCEDURES</b>	<b>8</b>
3.1	ACCESS CONTROL	9
3.2	AWARENESS AND TRAINING	19
3.3	AUDIT AND ACCOUNTABILITY	21
3.4	CONFIGURATION MANAGEMENT	26
3.5	IDENTIFICATION AND AUTHENTICATION	31
3.6	INCIDENT RESPONSE	36
3.7	MAINTENANCE	38
3.8	MEDIA PROTECTION	41
3.9	PERSONNEL SECURITY	45
3.10	PHYSICAL PROTECTION	46
3.11	RISK ASSESSMENT	49
3.12	SECURITY ASSESSMENT	51
3.13	SYSTEM AND COMMUNICATIONS PROTECTION	53
3.14	SYSTEM AND INFORMATION INTEGRITY	61
<b>APPENDIX A</b>	<b>REFERENCES</b>	<b>65</b>
<b>APPENDIX B</b>	<b>GLOSSARY</b>	<b>67</b>
<b>APPENDIX C</b>	<b>ACRONYMS</b>	<b>75</b>
<b>APPENDIX D</b>	<b>ASSESSMENT METHODS</b>	<b>76</b>

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





## CHAPTER ONE

# INTRODUCTION

## THE NEED TO ASSESS CUI SECURITY REQUIREMENTS

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies. [Executive Order 13556](#) established a governmentwide Controlled Unclassified Information (CUI)<sup>1</sup> Program to standardize the way the executive branch handles unclassified information that requires protection. The implementing regulation for the CUI Program is [32 CFR part 2002](#), *Controlled Unclassified Information*. Only federal information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.<sup>2</sup> [NIST Special Publication 800-171](#), *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, specifies the security requirements to ensure the confidentiality of CUI.

### 1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide procedures for assessing the CUI requirements in [NIST Special Publication 800-171](#). Compliance with the security requirements is addressed in CUI guidance and the CUI Federal Acquisition Regulation (FAR)<sup>3</sup> or as supplemented by federal agencies (e.g., Department of Defense Federal Acquisition Regulation). Organizations can use the assessment procedures to generate evidence to support the assertion that the security requirements have been satisfied.

The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of the safeguards intended to meet the set of security requirements specified in NIST Special Publication 800-171. In this context, the information gathered and the evidence produced can be used by an organization to:

- Identify potential problems or shortfalls in the organization's security and risk management programs;
- Identify security weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- Prioritize risk mitigation decisions and activities;
- Confirm that identified security weaknesses and deficiencies in the system and in the environment of operation have been addressed; and
- Support continuous monitoring activities and provide information security situational awareness.

---

<sup>1</sup> *Controlled Unclassified Information* is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls, excluding information that is classified under [Executive Order 13526](#), *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

<sup>2</sup> The [CUI Registry](#) is the online repository for information, guidance, policy, and requirements on handling CUI.

<sup>3</sup> The CUI Executive Agent is actively engaged in the process of developing a FAR clause that will apply the requirements of the federal CUI regulation and [NIST Special Publication 800-171](#) to contractors.

The assessment procedures in this publication offer the flexibility to customize assessments based on organizational policies and requirements, known threat and vulnerability information, system and platform dependencies, operational considerations, and tolerance for risk.<sup>4</sup>

### THE SCOPE OF CUI SECURITY REQUIREMENT ASSESSMENTS

For the CUI security requirements in [NIST Special Publication 800-171](#), nonfederal organizations describe in a *system security plan*, how the specified requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the environment in which the system operates; how the requirements are implemented; and the relationships with or connections to other systems. The scope of the assessments conducted using the procedures described in this publication are guided and informed by the individual system security plans for the organizational systems processing, storing, or transmitting CUI. The assessments focus on the implementation and effectiveness of the safeguards intended to meet a fixed set of security requirements as defined in NIST Special Publication 800-171.

## 1.2 TARGET AUDIENCE

This publication serves system, information security, and privacy<sup>5</sup> professionals including individuals with:

- System development responsibilities (e.g., program managers, system developers, system owners, systems integrators, system security engineers);
- Information security assessment and monitoring responsibilities (e.g., system evaluators, assessors, independent verifiers/validators, auditors, analysts, system owners);
- Information security, privacy, risk management, governance, and oversight responsibilities (e.g., authorizing officials, chief information officers, chief privacy officers, chief information security officers, system managers, information security managers); and
- Information security implementation and operational responsibilities (e.g., system owners, information owners/stewards, mission and business owners, systems administrators, system security officers).

## 1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- [Chapter Two](#) describes the fundamental concepts associated with assessments of CUI security requirements including assessment procedures, methods, objects, and assurance cases that can be created using evidence produced during assessments.

<sup>4</sup> The term *risk* is used to mean risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. See [NIST Special Publication 800-39](#) for additional information on organizational risk management and risk tolerance.

<sup>5</sup> References to privacy in this publication are made *only* in the context of where security and privacy considerations overlap—that is, in the security objective of *confidentiality*, which generally supports privacy and the protection of personally identifiable information from unauthorized disclosure. [NIST Internal Report 8062](#) provides additional information on the overlapping and complementary nature of security and privacy disciplines.

- [Chapter Three](#) provides a catalog of assessment procedures for the fourteen families of CUI security requirements in NIST Special Publication 800-171, including assessment objectives and potential assessment methods and objects for each procedure.
- [Supporting appendices](#) provide additional assessment-related information including general references; definitions and terms; acronyms; and a description of the assessment methods used in assessment procedures.

## CHAPTER TWO

# THE FUNDAMENTALS

### BASIC CONCEPTS FOR ASSESSMENTS OF CUI SECURITY REQUIREMENTS

The CUI security requirements in [NIST Special Publication 800-171](#) are organized into fourteen families. Each family contains the requirements related to the general security topic of the family. Table 1 lists the CUI security requirement families addressed in this publication. The assessment procedures in [Chapter Three](#) are grouped by family designations to help ensure completeness and consistency of assessments.

**TABLE 1: CUI SECURITY REQUIREMENT FAMILIES**

FAMILY	FAMILY
<a href="#">Access Control</a>	<a href="#">Media Protection</a>
<a href="#">Awareness and Training</a>	<a href="#">Personnel Security</a>
<a href="#">Audit and Accountability</a>	<a href="#">Physical Protection</a>
<a href="#">Configuration Management</a>	<a href="#">Risk Assessment</a>
<a href="#">Identification and Authentication</a>	<a href="#">Security Assessment</a>
<a href="#">Incident Response</a>	<a href="#">System and Communications Protection</a>
<a href="#">Maintenance</a>	<a href="#">System and Information Integrity</a>

## 2.1 ASSESSMENT PROCEDURES

An assessment procedure consists of an assessment *objective* and a set of potential assessment *methods* and assessment *objects* that can be used to conduct the assessment. Each assessment objective includes a determination statement related to the CUI security requirement that is the subject of the assessment. The determination statements are linked to the content of the CUI security requirements to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to a security requirement produces assessment *findings*. These findings reflect, or are subsequently used, to help determine if the security requirement has been satisfied.

Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals. Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system. Mechanisms are the specific hardware, software, or firmware safeguards employed within a system. Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.

The assessment methods define the nature and the extent of the assessor’s actions. The methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain evidence. The interview method is the process of holding discussions with individuals or groups

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

of individuals to facilitate understanding, achieve clarification, or obtain evidence. And finally, the test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

The assessment methods described above have associated attributes of *depth* and *coverage*, which define the level of effort for the assessment. These attributes provide a means to define the rigor and scope of the assessment for the increased assurance of security requirements. A description of assessment methods and objects is provided in [Appendix D](#).<sup>6</sup> Figure 1 illustrates an example of an assessment procedure for CUI security requirement 3.1.3 from NIST Special Publication 800-171.

<b>3.1.3</b>	<b>SECURITY REQUIREMENT</b>	
	Control the flow of CUI in accordance with approved authorizations.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.1.3[a]</b>	<i>information flow control policies are defined.</i>
	<b>3.1.3[b]</b>	<i>methods and enforcement mechanisms for controlling the flow of CUI are defined.</i>
	<b>3.1.3[c]</b>	<i>designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.</i>
	<b>3.1.3[d]</b>	<i>authorizations for controlling the flow of CUI are defined.</i>
	<b>3.1.3[e]</b>	<i>approved authorizations for controlling the flow of CUI are enforced.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing information flow enforcement policy].</p>	

**FIGURE 1: ASSESSMENT PROCEDURE FOR CUI SECURITY REQUIREMENT**

Organizations are not expected to employ *all* assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.

<sup>6</sup> Additional information on assessment methods and objects and the attributes of depth and coverage is provided in [NIST Special Publication 800-53A](#).

## 2.2 ASSURANCE CASES

Building an effective assurance case for determining compliance to CUI security requirements is a process that involves compiling evidence from a variety of sources and conducting different types of activities during an assessment. An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system is true. For assessments conducted using the procedures in this publication, that claim is *compliance* with the security requirements specified in [NIST Special Publication 800-171](#). Assessors gather evidence during the assessment process to allow designated officials<sup>7</sup> to make objective determinations about compliance to the CUI security requirements. The evidence needed to make such determinations can be obtained from various sources including self-assessments, independent third-party assessments, or other types of assessments, depending on the needs of the organization establishing the requirements and the organization conducting the assessments.

For example, many technical security requirements are satisfied by security capabilities that are built in to commercial information technology products and systems. Product assessments are typically conducted by independent, third-party testing organizations.<sup>8</sup> These assessments examine the security functions of products and established configuration settings. Assessments can also be conducted to demonstrate compliance to industry, national, or international security standards as well as developer and vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in hundreds of thousands of systems, these types of assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the products.

Ultimately, evidence needed to determine compliance comes from the implementation of the selected safeguards to satisfy the CUI security requirements and from the assessments of that implementation. Assessors can build on previously developed materials that started with the specification of the organization's information security needs and is further developed during the design, development, and implementation of the system and system components. These materials, developed while implementing security throughout the life cycle of the system, provide the initial evidence for an assurance case.

Assessments can be conducted by systems developers, systems integrators, auditors, system owners, or the security staffs of organizations. The assessors or assessment teams bring together available information about the system such as the results from individual component product assessments. The assessors can conduct additional system-level assessments using the procedures and methods contained in this publication and based on the implementation information provided by the nonfederal organization in its system security plan. System assessments can be used to compile and evaluate the evidence needed by organizations to help determine the effectiveness of the safeguards implemented to protect CUI; the actions needed to mitigate security-related risks to the organization; and compliance to the CUI security requirements.

---

<sup>7</sup> A *designated official* is an official, either internal or external to the nonfederal organization, with the responsibility to determine organizational compliance to CUI security requirements.

<sup>8</sup> Examples include Common Criteria Testing Laboratories evaluating commercial IT products in accordance with ISO/IEC 15408 and Cryptographic Module Validation Program Testing Laboratories evaluating cryptographic modules in accordance with Federal Information Processing Standard (FIPS) 140.

### APPLICABLE CUI SECURITY REQUIREMENTS

The system security plan is used to describe how the organization meets or plans to meet the CUI security requirements. Any security requirements that are deemed *non-applicable* by the organization (e.g., no wireless capability in the system or the system component processing, storing, or transmitting CUI), are documented as such in the system security plan. Once the system security plan is completed, a security assessment plan can be developed using the assessment procedures described in Chapter Three and tailoring those procedures as needed. An assessment procedure is developed for every CUI security requirement that is applicable to the system, system component, or the organization. Conversely, security requirements that are deemed non-applicable in the system security plan are *not* assessed.



## CHAPTER THREE

# THE PROCEDURES

### ASSESSMENT PROCEDURES, METHODS, AND OBJECTS FOR CUI SECURITY REQUIREMENTS

This chapter provides assessment procedures for all CUI security requirements defined in [NIST Special Publication 800-171](#). The assessment procedures are organized into fourteen families. Organizations conducting CUI security requirement assessments can build their assessment plans using the information provided in the generic assessment procedures—selecting the specific assessment methods and objects that meet the organization’s needs. Organizations also have flexibility in defining the level of rigor and detail associated with the assessment based on the assurance requirements of the organization. [Appendix D](#) provides additional information on the different levels of rigor and detail for assessments.

The assessment objective defined for each assessment procedure is achieved by applying the designated assessment methods to the selected assessment objects and compiling/producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement contained within an assessment procedure produces one of the following findings: *satisfied* or *other than satisfied*. A finding of “satisfied” indicates that for the security requirement addressed by the determination statement, the assessment information obtained (i.e., the evidence collected) indicates that the assessment objective has been met producing a fully acceptable result. A finding of “other than satisfied” indicates that for the security requirement addressed by the determination statement, the assessment findings obtained indicate potential anomalies that may need to be addressed by the organization. A finding of “other than satisfied” may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.

For assessment findings that are other than satisfied, organizations may define subcategories of findings indicating the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects of those weaknesses or deficiencies on organizational missions and/or business functions. Defining such subcategories can help to establish priorities for needed risk mitigation actions.

#### CAUTIONARY NOTE

The content in this publication can be used for many different assessment-related purposes in determining organizational compliance to the CUI security requirements. The broad range of potential assessment methods and objects listed in this publication do not necessarily reflect, and should not be directly associated with, actual compliance or noncompliance. Rather, the selection of specific assessment methods and objects from the list provided, can help generate a picture of overall compliance with the CUI security requirements. There is no expectation about the number of methods or objects needed to determine compliance to the CUI security requirements. Moreover, the entire list of potential assessment objects should not be viewed as required artifacts needed to determine compliance to the requirements. Organizations have the flexibility to determine the specific methods and objects sufficient to obtain the needed evidence to support claims of compliance.

### 3.1 ACCESS CONTROL

<b>3.1.1</b>	<b>SECURITY REQUIREMENT</b> Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.1.1[a]</b>   <i>authorized users are identified.</i>
	<b>3.1.1[b]</b>   <i>processes acting on behalf of authorized users are identified.</i>
	<b>3.1.1[c]</b>   <i>devices (and other systems) authorized to connect to the system are identified.</i>
	<b>3.1.1[d]</b>   <i>system access is limited to authorized users.</i>
	<b>3.1.1[e]</b>   <i>system access is limited to processes acting on behalf of authorized users.</i>
	<b>3.1.1[f]</b>   <i>system access is limited to authorized devices (including other systems).</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

<b>3.1.2</b>	<b>SECURITY REQUIREMENT</b> Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.1.2[a]</b>   <i>the types of transactions and functions that authorized users are permitted to execute are defined.</i>
	<b>3.1.2[b]</b>   <i>system access is limited to the defined types of transactions and functions for authorized users.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers]. <b>Test:</b> [SELECT FROM: Mechanisms implementing access control policy].

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

<b>3.1.3</b>	<b>SECURITY REQUIREMENT</b>	
	Control the flow of CUI in accordance with approved authorizations.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.1.3[a]</b>	<i>information flow control policies are defined.</i>
	<b>3.1.3[b]</b>	<i>methods and enforcement mechanisms for controlling the flow of CUI are defined.</i>
	<b>3.1.3[c]</b>	<i>designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.</i>
	<b>3.1.3[d]</b>	<i>authorizations for controlling the flow of CUI are defined.</i>
	<b>3.1.3[e]</b>	<i>approved authorizations for controlling the flow of CUI are enforced.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing information flow enforcement policy].</p>	

<b>3.1.4</b>	<b>SECURITY REQUIREMENT</b>	
	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.1.4[a]</b>	<i>the duties of individuals requiring separation are defined.</i>
	<b>3.1.4[b]</b>	<i>responsibilities for duties that require separation are assigned to separate individuals.</i>
	<b>3.1.4[c]</b>	<i>access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing separation of duties policy].</p>	

<b>3.1.5</b>	<b>SECURITY REQUIREMENT</b>	
	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.1.5[a]</b>	<i>privileged accounts are identified.</i>
	<b>3.1.5[b]</b>	<i>access to privileged accounts is authorized in accordance with the principle of least privilege.</i>
	<b>3.1.5[c]</b>	<i>security functions are identified.</i>
	<b>3.1.5[d]</b>	<i>access to security functions is authorized in accordance with the principle of least privilege.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring/audit records; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access is to be explicitly authorized; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities; personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management; mechanisms implementing least privilege functions; mechanisms prohibiting privileged access to the system].</p>	

<b>3.1.6</b>	<b>SECURITY REQUIREMENT</b>	
	Use non-privileged accounts or roles when accessing nonsecurity functions.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.1.6[a]</b>	<i>nonsecurity functions are identified.</i>
	<b>3.1.6[b]</b>	<i>users are required to use non-privileged accounts or roles when accessing nonsecurity functions.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing least privilege; system security plan; list of system-generated security functions assigned to system accounts or roles; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for defining least privileges necessary to accomplish specified organizational tasks; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing least privilege functions].</p>	

<b>3.1.7</b>	<b>SECURITY REQUIREMENT</b> Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.7[a]</b>	<i>privileged functions are defined.</i>
	<b>3.1.7[b]</b>	<i>non-privileged users are defined.</i>
	<b>3.1.7[c]</b>	<i>non-privileged users are prevented from executing privileged functions.</i>
	<b>3.1.7[d]</b>	<i>the execution of privileged functions is captured in audit logs.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing least privilege; system security plan; system design documentation; list of privileged functions and associated user account assignments; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; personnel with information security responsibilities; system developers]. <b>Test:</b> [SELECT FROM: Mechanisms implementing least privilege functions for non-privileged users; mechanisms auditing the execution of privileged functions].	

<b>3.1.8</b>	<b>SECURITY REQUIREMENT</b> Limit unsuccessful logon attempts.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.8[a]</b>	<i>the means of limiting unsuccessful logon attempts is defined.</i>
	<b>3.1.8[b]</b>	<i>the defined means of limiting unsuccessful logon attempts is implemented.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with information security responsibilities; system developers; system or network administrators]. <b>Test:</b> [SELECT FROM: Mechanisms implementing access control policy for unsuccessful logon attempts].	

<b>3.1.9</b>	<b>SECURITY REQUIREMENT</b> Provide privacy and security notices consistent with applicable CUI rules.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.9[a]</b>	<i>privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.</i>

<b>3.1.9[b]</b>	<i>privacy and security notices are displayed.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing system use notification].</p>	

<b>3.1.10</b>	<b>SECURITY REQUIREMENT</b> Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
<b>3.1.10[a]</b>	<i>the period of inactivity after which the system initiates a session lock is defined.</i>
<b>3.1.10[b]</b>	<i>access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.</i>
<b>3.1.10[c]</b>	<i>previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing access control policy for session lock].</p>	

<b>3.1.11</b>	<b>SECURITY REQUIREMENT</b> Terminate (automatically) a user session after a defined condition.
<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
<b>3.1.11[a]</b>	<i>conditions requiring a user session to terminate are defined.</i>
<b>3.1.11[b]</b>	<i>a user session is automatically terminated after any of the defined conditions occur.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing session termination; system design documentation; system security plan; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit logs and records; other relevant documents or records].</p>	

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

	<p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing user session termination].</p>
--	---

<b>3.1.12</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Monitor and control remote access sessions.</p>								
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p><i>Determine if:</i></p>								
	<table border="1" style="width: 100%;"> <tr> <td style="width: 15%; background-color: #1a3d4d; color: white;"><b>3.1.12[a]</b></td> <td><i>remote access sessions are permitted.</i></td> </tr> <tr> <td style="background-color: #1a3d4d; color: white;"><b>3.1.12[b]</b></td> <td><i>the types of permitted remote access are identified.</i></td> </tr> <tr> <td style="background-color: #1a3d4d; color: white;"><b>3.1.12[c]</b></td> <td><i>remote access sessions are controlled.</i></td> </tr> <tr> <td style="background-color: #1a3d4d; color: white;"><b>3.1.12[d]</b></td> <td><i>remote access sessions are monitored.</i></td> </tr> </table>	<b>3.1.12[a]</b>	<i>remote access sessions are permitted.</i>	<b>3.1.12[b]</b>	<i>the types of permitted remote access are identified.</i>	<b>3.1.12[c]</b>	<i>remote access sessions are controlled.</i>	<b>3.1.12[d]</b>	<i>remote access sessions are monitored.</i>
<b>3.1.12[a]</b>	<i>remote access sessions are permitted.</i>								
<b>3.1.12[b]</b>	<i>the types of permitted remote access are identified.</i>								
<b>3.1.12[c]</b>	<i>remote access sessions are controlled.</i>								
<b>3.1.12[d]</b>	<i>remote access sessions are monitored.</i>								
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; remote access authorizations; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for managing remote access connections; system or network administrators; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Remote access management capability for the system].</p>								

<b>3.1.13</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.</p>				
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p><i>Determine if:</i></p>				
	<table border="1" style="width: 100%;"> <tr> <td style="width: 15%; background-color: #1a3d4d; color: white;"><b>3.1.13[a]</b></td> <td><i>cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.</i></td> </tr> <tr> <td style="background-color: #1a3d4d; color: white;"><b>3.1.13[b]</b></td> <td><i>cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.</i></td> </tr> </table>	<b>3.1.13[a]</b>	<i>cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.</i>	<b>3.1.13[b]</b>	<i>cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.</i>
<b>3.1.13[a]</b>	<i>cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.</i>				
<b>3.1.13[b]</b>	<i>cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.</i>				
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].</p> <p><b>Test:</b> [SELECT FROM: Cryptographic mechanisms protecting remote access sessions].</p>				

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

<b>3.1.14</b>	<b>SECURITY REQUIREMENT</b> Route remote access via managed access control points.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.14[a]</b>	<i>managed access control points are identified and implemented.</i>
	<b>3.1.14[b]</b>	<i>remote access is routed through managed network access control points.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; list of all managed network access control points; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms routing all remote accesses through managed network access control points].</p>	

<b>3.1.15</b>	<b>SECURITY REQUIREMENT</b> Authorize remote execution of privileged commands and remote access to security-relevant information.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.15[a]</b>	<i>privileged commands authorized for remote execution are identified.</i>
	<b>3.1.15[b]</b>	<i>security-relevant information authorized to be accessed remotely is identified.</i>
	<b>3.1.15[c]</b>	<i>the execution of the identified privileged commands via remote access is authorized.</i>
	<b>3.1.15[d]</b>	<i>access to the identified security-relevant information via remote access is authorized.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing remote access to the system; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing remote access management].</p>		

<b>3.1.16</b>	<b>SECURITY REQUIREMENT</b> Authorize wireless access prior to allowing such connections.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.16[a]</b>	<i>wireless access points are identified.</i>
	<b>3.1.16[b]</b>	<i>wireless access is authorized prior to allowing such connections.</i>



<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>
<p><b>Examine:</b> [SELECT FROM: Access control policy; configuration management plan; procedures addressing wireless access implementation and usage (including restrictions); system security plan; system design documentation; system configuration settings and associated documentation; wireless access authorizations; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for managing wireless access connections; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Wireless access management capability for the system].</p>

<b>3.1.17</b>	<b>SECURITY REQUIREMENT</b>
Protect wireless access using authentication and encryption.	
<b>ASSESSMENT OBJECTIVE</b>	
Determine if:	
<b>3.1.17[a]</b>	<i>wireless access to the system is protected using authentication.</i>
<b>3.1.17[b]</b>	<i>wireless access to the system is protected using encryption.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Access control policy; system design documentation; procedures addressing wireless implementation and usage (including restrictions); system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing wireless access protections to the system].</p>	

<b>3.1.18</b>	<b>SECURITY REQUIREMENT</b>
Control connection of mobile devices.	
<b>ASSESSMENT OBJECTIVE</b>	
Determine if:	
<b>3.1.18[a]</b>	<i>mobile devices that process, store, or transmit CUI are identified.</i>
<b>3.1.18[b]</b>	<i>mobile device connections are authorized.</i>
<b>3.1.18[c]</b>	<i>mobile device connections are monitored and logged.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Access control policy; authorizations for mobile device connections to organizational systems; procedures addressing access control for mobile device usage (including restrictions); system design documentation; configuration management plan; system security plan; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel using mobile devices to access organizational systems; system or network administrators; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Access control capability authorizing mobile device connections to organizational systems].</p>	

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

<b>3.1.19</b>	<b>SECURITY REQUIREMENT</b> Encrypt CUI on mobile devices and mobile computing platforms.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.19[a]</b>	<i>mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.</i>
	<b>3.1.19[b]</b>	<i>encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine:</u> [SELECT FROM: Access control policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings and associated documentation; encryption mechanisms and associated configuration documentation; system security plan; system audit logs and records; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: Personnel with access control responsibilities for mobile devices; system or network administrators; personnel with information security responsibilities]. <u>Test:</u> [SELECT FROM: Encryption mechanisms protecting confidentiality of information on mobile devices].	

<b>3.1.20</b>	<b>SECURITY REQUIREMENT</b> Verify and control/limit connections to and use of external systems.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.20[a]</b>	<i>connections to external systems are identified.</i>
	<b>3.1.20[b]</b>	<i>the use of external systems is identified.</i>
	<b>3.1.20[c]</b>	<i>connections to external systems are verified.</i>
	<b>3.1.20[d]</b>	<i>the use of external systems is verified.</i>
	<b>3.1.20[e]</b>	<i>connections to external systems are controlled/limited.</i>
	<b>3.1.20[f]</b>	<i>the use of external systems is controlled/limited.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine:</u> [SELECT FROM: Access control policy; procedures addressing the use of external systems; terms and conditions for external systems; system security plan; list of applications accessible from external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: Personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems; system or network administrators; personnel with information security responsibilities]. <u>Test:</u> [SELECT FROM: Mechanisms implementing terms and conditions on use of external systems].	

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

<b>3.1.21</b>	<b>SECURITY REQUIREMENT</b> Limit use of portable storage devices on external systems.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.21[a]</b>	<i>the use of portable storage devices containing CUI on external systems is identified and documented.</i>
	<b>3.1.21[b]</b>	<i>limits on the use of portable storage devices containing CUI on external systems are defined.</i>
	<b>3.1.21[c]</b>	<i>the use of portable storage devices containing CUI on external systems is limited as defined.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing the use of external systems; system security plan; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with responsibilities for restricting or prohibiting use of organization-controlled storage devices on external systems; system or network administrators; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Mechanisms implementing restrictions on use of portable storage devices].	

<b>3.1.22</b>	<b>SECURITY REQUIREMENT</b> Control CUI posted or processed on publicly accessible systems.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.1.22[a]</b>	<i>individuals authorized to post or process information on publicly accessible systems are identified.</i>
	<b>3.1.22[b]</b>	<i>procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.</i>
	<b>3.1.22[c]</b>	<i>a review process is in place prior to posting of any content to publicly accessible systems.</i>
	<b>3.1.22[d]</b>	<i>content on publicly accessible systems is reviewed to ensure that it does not include CUI.</i>
	<b>3.1.22[e]</b>	<i>mechanisms are in place to remove and address improper posting of CUI.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing publicly accessible content; system security plan; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs and records; security awareness training records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Mechanisms implementing management of publicly accessible content].	

### 3.2 AWARENESS AND TRAINING

<b>3.2.1</b>	<b>SECURITY REQUIREMENT</b>	
	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.2.1[a]</b>	<i>security risks associated with organizational activities involving CUI are identified.</i>
	<b>3.2.1[b]</b>	<i>policies, standards, and procedures related to the security of the system are identified.</i>
	<b>3.2.1[c]</b>	<i>managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.</i>
	<b>3.2.1[d]</b>	<i>managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms managing security awareness training; mechanisms managing role-based security training].</p>	

<b>3.2.2</b>	<b>SECURITY REQUIREMENT</b>	
	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.2.2[a]</b>	<i>information security-related duties, roles, and responsibilities are defined.</i>
	<b>3.2.2[b]</b>	<i>information security-related duties, roles, and responsibilities are assigned to designated personnel.</i>
	<b>3.2.2[c]</b>	<i>personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities</p>	

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

	<p>for security awareness training; personnel with information security responsibilities; personnel representing the general system user community].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms managing role-based security training; mechanisms managing security awareness training].</p>
--	--

<b>3.2.3</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Provide security awareness training on recognizing and reporting potential indicators of insider threat.</p>	
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p>Determine if:</p>	
	<b>3.2.3[a]</b>	<i>potential indicators associated with insider threats are identified.</i>
	<b>3.2.3[b]</b>	<i>security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.</i>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; insider threat policy and procedures; system security plan; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel that participate in security awareness training; personnel with responsibilities for basic security awareness training; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms managing insider threat training].</p>	

### 3.3 AUDIT AND ACCOUNTABILITY

<b>3.3.1</b>	<b>SECURITY REQUIREMENT</b> Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.3.1[a]</b> <i>audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.</i>
	<b>3.3.1[b]</b> <i>the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.</i>
	<b>3.3.1[c]</b> <i>audit records are created (generated).</i>
	<b>3.3.1[d]</b> <i>audit records, once created, contain the defined content.</i>
	<b>3.3.1[e]</b> <i>retention requirements for audit records are defined.</i>
	<b>3.3.1[f]</b> <i>audit records are retained as defined.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators]. <b>Test:</b> [SELECT FROM: Mechanisms implementing system audit logging].

<b>3.3.2</b>	<b>SECURITY REQUIREMENT</b> Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.3.2[a]</b> <i>the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.</i>
	<b>3.3.2[b]</b> <i>audit records, once created, contain the defined content.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Audit and accountability policy; procedures addressing audit records and event types; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing audit record generation; procedures addressing audit review, analysis, and reporting; reports of audit findings; system audit logs and records; system events; system incident reports; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators].

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

	<b>Test:</b> [SELECT FROM: Mechanisms implementing system audit logging].
--	---

<b>3.3.3</b>	<b>SECURITY REQUIREMENT</b> Review and update logged events.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.3.3[a]</b>	<i>a process for determining when to review logged events is defined.</i>
	<b>3.3.3[b]</b>	<i>event types being logged are reviewed in accordance with the defined review process.</i>
	<b>3.3.3[c]</b>	<i>event types being logged are updated based on the review.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: Audit and accountability policy; procedures addressing audit records and event types; system security plan; list of organization-defined event types to be logged; reviewed and updated records of logged event types; system audit logs and records; system incident reports; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities].	
	<b>Test:</b> [SELECT FROM: Mechanisms supporting review and update of logged event types].	

<b>3.3.4</b>	<b>SECURITY REQUIREMENT</b> Alert in the event of an audit logging process failure.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.3.4[a]</b>	<i>personnel or roles to be alerted in the event of an audit logging process failure are identified.</i>
	<b>3.3.4[b]</b>	<i>types of audit logging process failures for which alert will be generated are defined.</i>
	<b>3.3.4[c]</b>	<i>identified personnel or roles are alerted in the event of an audit logging process failure.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: Audit and accountability policy; procedures addressing response to audit logging processing failures; system design documentation; system security plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit logging processing failure; system incident reports; system audit logs and records; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers].	
	<b>Test:</b> [SELECT FROM: Mechanisms implementing system response to audit logging processing failures].	

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

<b>3.3.5</b>	<b>SECURITY REQUIREMENT</b>	
	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.3.5[a]</b>	<i>audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.</i>
	<b>3.3.5[b]</b>	<i>defined audit record review, analysis, and reporting processes are correlated.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: Audit and accountability policy; procedures addressing audit record review, analysis, and reporting; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing investigation of and response to suspicious activities; system audit logs and records across different repositories; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: Personnel with audit record review, analysis, and reporting responsibilities; personnel with information security responsibilities].	
	<b>Test:</b> [SELECT FROM: Mechanisms supporting analysis and correlation of audit records; mechanisms integrating audit review, analysis and reporting].	

<b>3.3.6</b>	<b>SECURITY REQUIREMENT</b>	
	Provide audit record reduction and report generation to support on-demand analysis and reporting.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.3.6[a]</b>	<i>an audit record reduction capability that supports on-demand analysis is provided.</i>
	<b>3.3.6[b]</b>	<i>a report generation capability that supports on-demand reporting is provided.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: Audit and accountability policy; procedures addressing audit record reduction and report generation; system design documentation; system security plan; system configuration settings and associated documentation; audit record reduction, review, analysis, and reporting tools; system audit logs and records; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: Personnel with audit record reduction and report generation responsibilities; personnel with information security responsibilities].	
	<b>Test:</b> [SELECT FROM: Audit record reduction and report generation capability].	

<b>3.3.7</b>	<b>SECURITY REQUIREMENT</b>	
	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.3.7[a]</b>	<i>internal system clocks are used to generate time stamps for audit records.</i>



	<b>3.3.7[b]</b>	<i>an authoritative source with which to compare and synchronize internal system clocks is specified.</i>
	<b>3.3.7[c]</b>	<i>internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine:</u> [SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: Personnel with information security responsibilities; system or network administrators; system developers]. <u>Test:</u> [SELECT FROM: Mechanisms implementing time stamp generation; mechanisms implementing internal information system clock synchronization].	

<b>3.3.8</b>	<b>SECURITY REQUIREMENT</b>	
	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.3.8[a]</b>	<i>audit information is protected from unauthorized access.</i>
	<b>3.3.8[b]</b>	<i>audit information is protected from unauthorized modification.</i>
	<b>3.3.8[c]</b>	<i>audit information is protected from unauthorized deletion.</i>
	<b>3.3.8[d]</b>	<i>audit logging tools are protected from unauthorized access.</i>
	<b>3.3.8[e]</b>	<i>audit logging tools are protected from unauthorized modification.</i>
	<b>3.3.8[f]</b>	<i>audit logging tools are protected from unauthorized deletion.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine:</u> [SELECT FROM: Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation, system audit logs and records; audit logging tools; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. <u>Test:</u> [SELECT FROM: Mechanisms implementing audit information protection].	

<b>3.3.9</b>	<b>SECURITY REQUIREMENT</b>	
	Limit management of audit logging functionality to a subset of privileged users.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.3.9[a]</b>	<i>a subset of privileged users granted access to manage audit logging functionality is defined.</i>
	<b>3.3.9[b]</b>	<i>management of audit logging functionality is limited to the defined subset of privileged users.</i>

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

**POTENTIAL ASSESSMENT METHODS AND OBJECTS**

**Examine:** [*SELECT FROM:* Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation; access authorizations; system-generated list of privileged users with access to management of audit logging functionality; access control list; system audit logs and records; other relevant documents or records].

**Interview:** [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers].

**Test:** [*SELECT FROM:* Mechanisms managing access to audit logging functionality].

### 3.4 CONFIGURATION MANAGEMENT

<b>3.4.1</b>	<b>SECURITY REQUIREMENT</b>	
	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.4.1[a]</b>	<i>a baseline configuration is established.</i>
	<b>3.4.1[b]</b>	<i>the baseline configuration includes hardware, software, firmware, and documentation.</i>
	<b>3.4.1[c]</b>	<i>the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.</i>
	<b>3.4.1[d]</b>	<i>a system inventory is established.</i>
	<b>3.4.1[e]</b>	<i>the system inventory includes hardware, software, firmware, and documentation.</i>
	<b>3.4.1[f]</b>	<i>the inventory is maintained (reviewed and updated) throughout the system development life cycle.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; procedures addressing system inventory; system security plan; configuration management plan; system inventory records; inventory review and update records; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system component installation records; system component removal records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organizational processes for updating inventory of system components; mechanisms supporting or implementing the system inventory; mechanisms implementing updating of the system inventory].</p>	

<b>3.4.2</b>	<b>SECURITY REQUIREMENT</b>	
	Establish and enforce security configuration settings for information technology products employed in organizational systems.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.4.2[a]</b>	<i>security configuration settings for information technology products employed in the system are established and included in the baseline configuration.</i>
	<b>3.4.2[b]</b>	<i>security configuration settings for information technology products employed in the system are enforced.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	

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

	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; baseline configuration; procedures addressing configuration settings for the system; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; evidence supporting approved deviations from established configuration settings; change control records; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings; processes for managing baseline configurations; mechanisms supporting configuration control of baseline configurations].</p>
--	--

<b>3.4.3</b>	<b>SECURITY REQUIREMENT</b>
Track, review, approve or disapprove, and log changes to organizational systems.	
<b>ASSESSMENT OBJECTIVE</b>	
<i>Determine if:</i>	
3.4.3[a]	<i>changes to the system are tracked.</i>
3.4.3[b]	<i>changes to the system are reviewed.</i>
3.4.3[c]	<i>changes to the system are approved or disapproved.</i>
3.4.3[d]	<i>changes to the system are logged.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; system security plan; change control records; system audit logs and records; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with configuration change control responsibilities; personnel with information security responsibilities; system or network administrators; members of change control board or similar].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for configuration change control; mechanisms that implement configuration change control].</p>	

<b>3.4.4</b>	<b>SECURITY REQUIREMENT</b>
Analyze the security impact of changes prior to implementation.	
<b>ASSESSMENT OBJECTIVE</b>	
<i>Determine if the security impact of changes to the system is analyzed prior to implementation.</i>	
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing security impact analysis for system changes; configuration management plan; security impact analysis documentation; system security plan; analysis tools and associated outputs; change control records; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibility for conducting security impact analysis; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for security impact analysis].</p>	

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

<b>3.4.5</b>	<b>SECURITY REQUIREMENT</b>	
	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.4.5[a]</b>	<i>physical access restrictions associated with changes to the system are defined.</i>
	<b>3.4.5[b]</b>	<i>physical access restrictions associated with changes to the system are documented.</i>
	<b>3.4.5[c]</b>	<i>physical access restrictions associated with changes to the system are approved.</i>
	<b>3.4.5[d]</b>	<i>physical access restrictions associated with changes to the system are enforced.</i>
	<b>3.4.5[e]</b>	<i>logical access restrictions associated with changes to the system are defined.</i>
	<b>3.4.5[f]</b>	<i>logical access restrictions associated with changes to the system are documented.</i>
	<b>3.4.5[g]</b>	<i>logical access restrictions associated with changes to the system are approved.</i>
	<b>3.4.5[h]</b>	<i>logical access restrictions associated with changes to the system are enforced.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; system security plan; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with logical access control responsibilities; personnel with physical access control responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for managing access restrictions associated with changes to the system; mechanisms supporting, implementing, and enforcing access restrictions associated with changes to the system].</p>	

<b>3.4.6</b>	<b>SECURITY REQUIREMENT</b>	
	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.4.6[a]</b>	<i>essential system capabilities are defined based on the principle of least functionality.</i>
	<b>3.4.6[b]</b>	<i>the system is configured to provide only the defined essential capabilities.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing least functionality in the system; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].</p>	

	<p><b>Interview:</b> [SELECT FROM: Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes prohibiting or restricting functions, ports, protocols, or services; mechanisms implementing restrictions or prohibition of functions, ports, protocols, or services].</p>
--	--

<b>3.4.7</b>	<b>SECURITY REQUIREMENT</b>
	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
	<b>ASSESSMENT OBJECTIVE</b>
	Determine if:
	<b>3.4.7[a]</b> <i>essential programs are defined.</i>
	<b>3.4.7[b]</b> <i>the use of nonessential programs is defined.</i>
	<b>3.4.7[c]</b> <i>the use of nonessential programs is restricted, disabled, or prevented as defined.</i>
	<b>3.4.7[d]</b> <i>essential functions are defined.</i>
	<b>3.4.7[e]</b> <i>the use of nonessential functions is defined.</i>
	<b>3.4.7[f]</b> <i>the use of nonessential functions is restricted, disabled, or prevented as defined.</i>
	<b>3.4.7[g]</b> <i>essential ports are defined.</i>
	<b>3.4.7[h]</b> <i>the use of nonessential ports is defined.</i>
	<b>3.4.7[i]</b> <i>the use of nonessential ports is restricted, disabled, or prevented as defined.</i>
	<b>3.4.7[j]</b> <i>essential protocols are defined.</i>
	<b>3.4.7[k]</b> <i>the use of nonessential protocols is defined.</i>
	<b>3.4.7[l]</b> <i>the use of nonessential protocols is restricted, disabled, or prevented as defined.</i>
	<b>3.4.7[m]</b> <i>essential services are defined.</i>
	<b>3.4.7[n]</b> <i>the use of nonessential services is defined.</i>
	<b>3.4.7[o]</b> <i>the use of nonessential services is restricted, disabled, or prevented as defined.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>
	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system security plan; system design documentation; security configuration checklists; system configuration settings and associated documentation; specifications for preventing software program execution; documented reviews of programs, functions, ports, protocols, and/or services; change control records; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for reviewing programs, functions, ports, protocols, and services on the system; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services; mechanisms implementing review and handling of nonessential programs, functions, ports, protocols, or services; organizational processes preventing program execution on the system; organizational processes for software program usage and restrictions; mechanisms supporting or implementing software program usage and restrictions; mechanisms preventing program execution on the system].</p>

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

<b>3.4.8</b>	<b>SECURITY REQUIREMENT</b>	
	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.4.8[a]</b>	<i>a policy specifying whether whitelisting or blacklisting is to be implemented is specified.</i>
	<b>3.4.8[b]</b>	<i>the software allowed to execute under whitelisting or denied use under blacklisting is specified.</i>
	<b>3.4.8[c]</b>	<i>whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; system security plan; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs not authorized to execute on the system; list of software programs authorized to execute on the system; security configuration checklists; review and update records associated with list of authorized or unauthorized software programs; change control records; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for identifying software authorized or not authorized to execute on the system; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational process for identifying, reviewing, and updating programs authorized or not authorized to execute on the system; process for implementing blacklisting or whitelisting; mechanisms supporting or implementing blacklisting or whitelisting].</p>	

<b>3.4.9</b>	<b>SECURITY REQUIREMENT</b>	
	Control and monitor user-installed software.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.4.9[a]</b>	<i>a policy for controlling the installation of software by users is established.</i>
	<b>3.4.9[b]</b>	<i>installation of software by users is controlled based on the established policy.</i>
	<b>3.4.9[c]</b>	<i>installation of software by users is monitored.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Configuration management policy; procedures addressing user installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user-installed software; system monitoring records; system audit logs and records; continuous monitoring strategy; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibilities for governing user-installed software; personnel operating, using, or maintaining the system; personnel monitoring compliance with user-installed software policy; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes governing user-installed software on the system; mechanisms enforcing rules or methods for governing the installation of software by users; mechanisms monitoring policy compliance].</p>	

### 3.5 IDENTIFICATION AND AUTHENTICATION

<b>3.5.1</b>	<b>SECURITY REQUIREMENT</b> Identify system users, processes acting on behalf of users, and devices.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.5.1[a]</b>	<i>system users are identified.</i>
	<b>3.5.1[b]</b>	<i>processes acting on behalf of users are identified.</i>
	<b>3.5.1[c]</b>	<i>devices accessing the system are identified.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers]. <b>Test:</b> [SELECT FROM: Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability].	

<b>3.5.2</b>	<b>SECURITY REQUIREMENT</b> Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.5.2[a]</b>	<i>the identity of each user is authenticated or verified as a prerequisite to system access.</i>
	<b>3.5.2[b]</b>	<i>the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.</i>
	<b>3.5.2[c]</b>	<i>the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators]. <b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing authenticator management capability].	

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



<b>3.5.3</b>	<b>SECURITY REQUIREMENT</b> Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.5.3[a]</b>	<i>privileged accounts are identified.</i>
	<b>3.5.3[b]</b>	<i>multifactor authentication is implemented for local access to privileged accounts.</i>
	<b>3.5.3[c]</b>	<i>multifactor authentication is implemented for network access to privileged accounts.</i>
	<b>3.5.3[d]</b>	<i>multifactor authentication is implemented for network access to non-privileged accounts.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>		
<p><b>Examine:</b> [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing multifactor authentication capability].</p>		

<b>3.5.4</b>	<b>SECURITY REQUIREMENT</b> Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.</i>	
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of privileged system accounts; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing identification and authentication capability or replay resistant authentication mechanisms].</p>	

<b>3.5.5</b>	<b>SECURITY REQUIREMENT</b> Prevent reuse of identifiers for a defined period.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.5.5[a]</b>	<i>a period within which identifiers cannot be reused is defined.</i>

	<b>3.5.5[b]</b>	<i>reuse of identifiers is prevented within the defined period.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine</u> : [SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records]. <u>Interview</u> : [SELECT FROM: Personnel with identifier management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. <u>Test</u> : [SELECT FROM: Mechanisms supporting or implementing identifier management].	

<b>3.5.6</b>	<b>SECURITY REQUIREMENT</b>	
	Disable identifiers after a defined period of inactivity.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.5.6[a]</b>	<i>a period of inactivity after which an identifier is disabled is defined.</i>
	<b>3.5.6[b]</b>	<i>identifiers are disabled after the defined period of inactivity.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine</u> : [SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records]. <u>Interview</u> : [SELECT FROM: Personnel with identifier management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. <u>Test</u> : [SELECT FROM: Mechanisms supporting or implementing identifier management].	

<b>3.5.7</b>	<b>SECURITY REQUIREMENT</b>	
	Enforce a minimum password complexity and change of characters when new passwords are created.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.5.7[a]</b>	<i>password complexity requirements are defined.</i>
	<b>3.5.7[b]</b>	<i>password change of character requirements are defined.</i>
	<b>3.5.7[c]</b>	<i>minimum password complexity requirements as defined are enforced when new passwords are created.</i>
	<b>3.5.7[d]</b>	<i>minimum password change of character requirements as defined are enforced when new passwords are created.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <u>Examine</u> : [SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records].	

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

	<p><b>Interview:</b> [SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing password-based authenticator management capability].</p>
--	---

<b>3.5.8</b>	<b>SECURITY REQUIREMENT</b>
Prohibit password reuse for a specified number of generations.	
<b>ASSESSMENT OBJECTIVE</b>	
<i>Determine if:</i>	
<b>3.5.8[a]</b>	<i>the number of generations during which a password cannot be reused is specified.</i>
<b>3.5.8[b]</b>	<i>reuse of passwords is prohibited during the specified number of generations.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; password configurations and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing password-based authenticator management capability].</p>	

<b>3.5.9</b>	<b>SECURITY REQUIREMENT</b>
Allow temporary password use for system logons with an immediate change to a permanent password.	
<b>ASSESSMENT OBJECTIVE</b>	
<i>Determine if an immediate change to a permanent password is required when a temporary password is used for system logon.</i>	
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing password-based authenticator management capability].</p>	

<b>3.5.10</b>	<b>SECURITY REQUIREMENT</b>
Store and transmit only cryptographically-protected passwords.	
<b>ASSESSMENT OBJECTIVE</b>	
<i>Determine if:</i>	

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

<b>3.5.10</b>	<b>3.5.10[a]</b>	<i>passwords are cryptographically protected in storage.</i>
	<b>3.5.10[b]</b>	<i>passwords are cryptographically protected in transit.</i>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing password-based authenticator management capability].</p>	

<b>3.5.11</b>	<b>SECURITY REQUIREMENT</b>	
	Obscure feedback of authentication information.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if authentication information is obscured during the authentication process.</i>	
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Identification and authentication policy; procedures addressing authenticator feedback; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with information security responsibilities; system or network administrators; system developers].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing the obscuring of feedback of authentication information during authentication].</p>	

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

### 3.6 INCIDENT RESPONSE

<b>3.6.1</b>	<b>SECURITY REQUIREMENT</b>	
	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.6.1[a]</b>	<i>an operational incident-handling capability is established.</i>
	<b>3.6.1[b]</b>	<i>the operational incident-handling capability includes preparation.</i>
	<b>3.6.1[c]</b>	<i>the operational incident-handling capability includes detection.</i>
	<b>3.6.1[d]</b>	<i>the operational incident-handling capability includes analysis.</i>
	<b>3.6.1[e]</b>	<i>the operational incident-handling capability includes containment.</i>
	<b>3.6.1[f]</b>	<i>the operational incident-handling capability includes recovery.</i>
	<b>3.6.1[g]</b>	<i>the operational incident-handling capability includes user response activities.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing incident response assistance; incident response plan; contingency plan; system security plan; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response training records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with incident response assistance and support responsibilities; personnel with access to incident response support and assistance capability; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Incident-handling capability for the organization; organizational processes for incident response assistance; mechanisms supporting or implementing incident response assistance].</p>	

<b>3.6.2</b>	<b>SECURITY REQUIREMENT</b>	
	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.6.2[a]</b>	<i>incidents are tracked.</i>
	<b>3.6.2[b]</b>	<i>incidents are documented.</i>
	<b>3.6.2[c]</b>	<i>authorities to whom incidents are to be reported are identified.</i>
	<b>3.6.2[d]</b>	<i>organizational officials to whom incidents are to be reported are identified.</i>
	<b>3.6.2[e]</b>	<i>identified authorities are notified of incidents.</i>
	<b>3.6.2[f]</b>	<i>identified organizational officials are notified of incidents.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	

	<p><b>Examine:</b> [SELECT FROM: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; system security plan; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with incident monitoring responsibilities; personnel with incident reporting responsibilities; personnel who have or should have reported incidents; personnel (authorities) to whom incident information is to be reported; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Incident monitoring capability for the organization; mechanisms supporting or implementing tracking and documenting of system security incidents; organizational processes for incident reporting; mechanisms supporting or implementing incident reporting].</p>
--	---

<b>3.6.3</b>	<p><b>SECURITY REQUIREMENT</b> Test the organizational incident response capability.</p>
	<p><b>ASSESSMENT OBJECTIVE</b> <i>Determine if the incident response capability is tested.</i></p>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with incident response testing responsibilities; personnel with information security responsibilities; personnel with responsibilities for testing plans related to incident response].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms and processes for incident response].</p>

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

### 3.7 MAINTENANCE

<b>3.7.1</b>	<b>SECURITY REQUIREMENT</b> Perform maintenance on organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if system maintenance is performed.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. <b>Test:</b> [SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

<b>3.7.2</b>	<b>SECURITY REQUIREMENT</b> Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.7.2[a]</b>   <i>tools used to conduct system maintenance are controlled.</i>
	<b>3.7.2[b]</b>   <i>techniques used to conduct system maintenance are controlled.</i>
	<b>3.7.2[c]</b>   <i>mechanisms used to conduct system maintenance are controlled.</i>
	<b>3.7.2[d]</b>   <i>personnel used to conduct system maintenance are controlled.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

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

<b>3.7.3</b>	<b>SECURITY REQUIREMENT</b> Ensure equipment removed for off-site maintenance is sanitized of any CUI.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. <b>Test:</b> [SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

<b>3.7.4</b>	<b>SECURITY REQUIREMENT</b> Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

<b>3.7.5</b>	<b>SECURITY REQUIREMENT</b> Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.				
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>				
	<table border="1" style="width: 100%;"> <tr> <td style="width: 15%;"><b>3.7.5[a]</b></td> <td><i>multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.</i></td> </tr> <tr> <td><b>3.7.5[b]</b></td> <td><i>nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.</i></td> </tr> </table>	<b>3.7.5[a]</b>	<i>multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.</i>	<b>3.7.5[b]</b>	<i>nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.</i>
<b>3.7.5[a]</b>	<i>multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.</i>				
<b>3.7.5[b]</b>	<i>nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.</i>				
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System maintenance policy; procedures addressing nonlocal system maintenance; system security plan; system design documentation; system configuration				



	<p>settings and associated documentation; maintenance records; diagnostic records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for managing nonlocal maintenance; mechanisms implementing, supporting, and managing nonlocal maintenance; mechanisms for strong authentication of nonlocal maintenance diagnostic sessions; mechanisms for terminating nonlocal maintenance sessions and network connections].</p>
--	---

<b>3.7.6</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Supervise the maintenance activities of maintenance personnel without required access authorization.</p>
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p><i>Determine if maintenance personnel without required access authorization are supervised during maintenance activities.</i></p>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: System maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel].</p>

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

### 3.8 MEDIA PROTECTION

<b>3.8.1</b>	<b>SECURITY REQUIREMENT</b>	
	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.8.1[a]</b>	<i>paper media containing CUI is physically controlled.</i>
	<b>3.8.1[b]</b>	<i>digital media containing CUI is physically controlled.</i>
	<b>3.8.1[c]</b>	<i>paper media containing CUI is securely stored.</i>
	<b>3.8.1[d]</b>	<i>digital media containing CUI is securely stored.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].</p>	

<b>3.8.2</b>	<b>SECURITY REQUIREMENT</b>	
	Limit access to CUI on system media to authorized users.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if access to CUI on system media is limited to authorized users.</i>	
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].</p>	

<b>3.8.3</b>	<b>SECURITY REQUIREMENT</b>	
	Sanitize or destroy system media containing CUI before disposal or release for reuse.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.8.3[a]</b>	<i>system media containing CUI is sanitized or destroyed before disposal.</i>
	<b>3.8.3[b]</b>	<i>system media containing CUI is sanitized before it is released for reuse.</i>

<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>
<p><b>Examine:</b> [SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; applicable standards and policies addressing media sanitization; system security plan; media sanitization records; system audit logs and records; system design documentation; system configuration settings and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with media sanitization responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for media sanitization; mechanisms supporting or implementing media sanitization].</p>

<b>3.8.4</b>	<b>SECURITY REQUIREMENT</b>
Mark media with necessary CUI markings and distribution limitations.	
<b>ASSESSMENT OBJECTIVE</b>	
Determine if:	
<b>3.8.4[a]</b>	<i>media containing CUI is marked with applicable CUI markings.</i>
<b>3.8.4[b]</b>	<i>media containing CUI is marked with distribution limitations.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: System media protection policy; procedures addressing media marking; physical and environmental protection policy and procedures; system security plan; list of system media marking security attributes; designated controlled areas; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system media protection and marking responsibilities; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for marking information media; mechanisms supporting or implementing media marking].</p>	

<b>3.8.5</b>	<b>SECURITY REQUIREMENT</b>
Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
<b>ASSESSMENT OBJECTIVE</b>	
Determine if:	
<b>3.8.5[a]</b>	<i>access to media containing CUI is controlled.</i>
<b>3.8.5[b]</b>	<i>accountability for media containing CUI is maintained during transport outside of controlled areas.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing media storage and media protection].</p>	

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

<b>3.8.6</b>	<b>SECURITY REQUIREMENT</b> Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings and associated documentation; system media transport records; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system media transport responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas].

<b>3.8.7</b>	<b>SECURITY REQUIREMENT</b> Control the use of removable media on system components.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if the use of removable media on system components is controlled.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators]. <b>Test:</b> [SELECT FROM: Organizational processes for media use; mechanisms restricting or prohibiting use of system media on systems or system components].

<b>3.8.8</b>	<b>SECURITY REQUIREMENT</b> Prohibit the use of portable storage devices when such devices have no identifiable owner.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system configuration settings and associated documentation; system design documentation; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators]. <b>Test:</b> [SELECT FROM: Organizational processes for media use; mechanisms prohibiting use of media on systems or system components].

<b>3.8.9</b>	<b>SECURITY REQUIREMENT</b> Protect the confidentiality of backup CUI at storage locations.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if the confidentiality of backup CUI is protected at storage locations.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [ <i>SELECT FROM:</i> Procedures addressing system backup; system configuration settings and associated documentation; security plan; backup storage locations; system backup logs or records; other relevant documents or records]. <b>Interview:</b> [ <i>SELECT FROM:</i> Personnel with system backup responsibilities; personnel with information security responsibilities]. <b>Test:</b> [ <i>SELECT FROM:</i> Organizational processes for conducting system backups; mechanisms supporting or implementing system backups].

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

### 3.9 PERSONNEL SECURITY

<b>3.9.1</b>	<b>SECURITY REQUIREMENT</b> Screen individuals prior to authorizing access to organizational systems containing CUI.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with personnel security responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for personnel screening].

<b>3.9.2</b>	<b>SECURITY REQUIREMENT</b> Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.9.2[a]</b> <i>a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.</i>
	<b>3.9.2[b]</b> <i>system access and credentials are terminated consistent with personnel actions such as termination or transfer.</i>
	<b>3.9.2[c]</b> <i>the system is protected during and after personnel transfer actions.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked authenticators and credentials; records of exit interviews; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with personnel security responsibilities; personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for personnel transfer and termination; mechanisms supporting or implementing personnel transfer and termination notifications; mechanisms for disabling system access and revoking authenticators].

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

### 3.10 PHYSICAL PROTECTION

<b>3.10.1</b>	<b>SECURITY REQUIREMENT</b> Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.10.1[a]</b> <i>authorized individuals allowed physical access are identified.</i>
	<b>3.10.1[b]</b> <i>physical access to organizational systems is limited to authorized individuals.</i>
	<b>3.10.1[c]</b> <i>physical access to equipment is limited to authorized individuals.</i>
	<b>3.10.1[d]</b> <i>physical access to operating environments is limited to authorized individuals.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations].

<b>3.10.2</b>	<b>SECURITY REQUIREMENT</b> Protect and monitor the physical facility and support infrastructure for organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.10.2[a]</b> <i>the physical facility where organizational systems reside is protected.</i>
	<b>3.10.2[b]</b> <i>the support infrastructure for organizational systems is protected.</i>
	<b>3.10.2[c]</b> <i>the physical facility where organizational systems reside is monitored.</i>
	<b>3.10.2[d]</b> <i>the support infrastructure for organizational systems is monitored.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; system security plan; physical access logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for monitoring physical access; mechanisms supporting or implementing physical access monitoring; mechanisms supporting or implementing the review of physical access logs].

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

<b>3.10.3</b>	<b>SECURITY REQUIREMENT</b> Escort visitors and monitor visitor activity.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.10.3[a]</b>   <i>visitors are escorted.</i>
	<b>3.10.3[b]</b>   <i>visitor activity is monitored.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with physical access control responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

<b>3.10.4</b>	<b>SECURITY REQUIREMENT</b> Maintain audit logs of physical access.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if audit logs of physical access are maintained.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with physical access control responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

<b>3.10.5</b>	<b>SECURITY REQUIREMENT</b> Control and manage physical access devices.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.10.5[a]</b>   <i>physical access devices are identified.</i>
	<b>3.10.5[b]</b>   <i>physical access devices are controlled.</i>
	<b>3.10.5[c]</b>   <i>physical access devices are managed.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records;



	<p>inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with physical access control responsibilities; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].</p>
--	---

<b>3.10.6</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Enforce safeguarding measures for CUI at alternate work sites.</p>				
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p><i>Determine if:</i></p>				
	<table border="1" style="width: 100%;"> <tr> <td style="width: 15%;"><b>3.10.6[a]</b></td> <td><i>safeguarding measures for CUI are defined for alternate work sites.</i></td> </tr> <tr> <td><b>3.10.6[b]</b></td> <td><i>safeguarding measures for CUI are enforced for alternate work sites.</i></td> </tr> </table>	<b>3.10.6[a]</b>	<i>safeguarding measures for CUI are defined for alternate work sites.</i>	<b>3.10.6[b]</b>	<i>safeguarding measures for CUI are enforced for alternate work sites.</i>
<b>3.10.6[a]</b>	<i>safeguarding measures for CUI are defined for alternate work sites.</i>				
<b>3.10.6[b]</b>	<i>safeguarding measures for CUI are enforced for alternate work sites.</i>				
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for personnel; system security plan; list of safeguards required for alternate work sites; assessments of safeguards at alternate work sites; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel].</p>				

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

### 3.11 RISK ASSESSMENT

<b>3.11.1</b>	<b>SECURITY REQUIREMENT</b> 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 CUI.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.11.1[a]</b> <i>the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.</i>
	<b>3.11.1[b]</b> <i>risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with risk assessment responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].

<b>3.11.2</b>	<b>SECURITY REQUIREMENT</b> Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.11.2[a]</b> <i>the frequency to scan for vulnerabilities in organizational systems and applications is defined.</i>
	<b>3.11.2[b]</b> <i>vulnerability scans are performed on organizational systems with the defined frequency.</i>
	<b>3.11.2[c]</b> <i>vulnerability scans are performed on applications with the defined frequency.</i>
	<b>3.11.2[d]</b> <i>vulnerability scans are performed on organizational systems when new vulnerabilities are identified.</i>
	<b>3.11.2[e]</b> <i>vulnerability scans are performed on applications when new vulnerabilities are identified.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].

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

	<p><b>Test:</b> [SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].</p>
--	---

<b>3.11.3</b>	<p><b>SECURITY REQUIREMENT</b> Remediate vulnerabilities in accordance with risk assessments.</p>
	<p><b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i></p>
<b>3.11.3[a]</b>	<i>vulnerabilities are identified.</i>
<b>3.11.3[b]</b>	<i>vulnerabilities are remediated in accordance with risk assessments.</i>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with information security responsibilities; system or network administrators].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].</p>

### 3.12 SECURITY ASSESSMENT

<b>3.12.1</b>	<b>SECURITY REQUIREMENT</b>	
	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.12.1[a]</b>	<i>the frequency of security control assessments is defined.</i>
	<b>3.12.1[b]</b>	<i>security controls are assessed with the defined frequency to determine if the controls are effective in their application.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: Personnel with security assessment responsibilities; personnel with information security responsibilities].	
	<b>Test:</b> [SELECT FROM: Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].	

<b>3.12.2</b>	<b>SECURITY REQUIREMENT</b>	
	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.12.2[a]</b>	<i>deficiencies and vulnerabilities to be addressed by the plan of action are identified.</i>
	<b>3.12.2[b]</b>	<i>a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.</i>
	<b>3.12.2[c]</b>	<i>the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities].	
	<b>Test:</b> [SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action].	

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

<b>3.12.3</b>	<b>SECURITY REQUIREMENT</b> Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Security planning policy; organizational procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

<b>3.12.4</b>	<b>SECURITY REQUIREMENT</b> Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.12.4[a]</b> <i>a system security plan is developed.</i>
	<b>3.12.4[b]</b> <i>the system boundary is described and documented in the system security plan.</i>
	<b>3.12.4[c]</b> <i>the system environment of operation is described and documented in the system security plan.</i>
	<b>3.12.4[d]</b> <i>the security requirements identified and approved by the designated authority as non-applicable are identified.</i>
	<b>3.12.4[e]</b> <i>the method of security requirement implementation is described and documented in the system security plan.</i>
	<b>3.12.4[f]</b> <i>the relationship with or connection to other systems is described and documented in the system security plan.</i>
	<b>3.12.4[g]</b> <i>the frequency to update the system security plan is defined.</i>
	<b>3.12.4[h]</b> <i>system security plan is updated with the defined frequency.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

### 3.13 SYSTEM AND COMMUNICATIONS PROTECTION

<b>3.13.1</b>	<b>SECURITY REQUIREMENT</b> Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.13.1[a]</b>   <i>the external system boundary is defined.</i>
	<b>3.13.1[b]</b>   <i>key internal system boundaries are defined.</i>
	<b>3.13.1[c]</b>   <i>communications are monitored at the external system boundary.</i>
	<b>3.13.1[d]</b>   <i>communications are monitored at key internal boundaries.</i>
	<b>3.13.1[e]</b>   <i>communications are controlled at the external system boundary.</i>
	<b>3.13.1[f]</b>   <i>communications are controlled at key internal boundaries.</i>
	<b>3.13.1[g]</b>   <i>communications are protected at the external system boundary.</i>
	<b>3.13.1[h]</b>   <i>communications are protected at key internal boundaries.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; enterprise security architecture documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. <b>Test:</b> [SELECT FROM: Mechanisms implementing boundary protection capability].

<b>3.13.2</b>	<b>SECURITY REQUIREMENT</b> Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.13.2[a]</b>   <i>architectural designs that promote effective information security are identified.</i>
	<b>3.13.2[b]</b>   <i>software development techniques that promote effective information security are identified.</i>
	<b>3.13.2[c]</b>   <i>systems engineering principles that promote effective information security are identified.</i>
	<b>3.13.2[d]</b>   <i>identified architectural designs that promote effective information security are employed.</i>
	<b>3.13.2[e]</b>   <i>identified software development techniques that promote effective information security are employed.</i>

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

<b>3.13.2[f]</b>	<i>identified systems engineering principles that promote effective information security are employed.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; system and communications protection policy; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; security architecture documentation; security requirements and specifications for the system; system design documentation; system configuration settings and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with responsibility for determining information system security requirements; personnel with information system design, development, implementation, and modification responsibilities; personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan; processes for applying security engineering principles in system specification, design, development, implementation, and modification; automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification].</p>	

<b>3.13.3</b>	<b>SECURITY REQUIREMENT</b> Separate user functionality from system management functionality.
<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
<b>3.13.3[a]</b>	<i>user functionality is identified.</i>
<b>3.13.3[b]</b>	<i>system management functionality is identified.</i>
<b>3.13.3[c]</b>	<i>user functionality is separated from system management functionality.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer].</p> <p><b>Test:</b> [SELECT FROM: Separation of user functionality from system management functionality].</p>	

<b>3.13.4</b>	<b>SECURITY REQUIREMENT</b> Prevent unauthorized and unintended information transfer via shared system resources.
<b>ASSESSMENT OBJECTIVE</b> <i>Determine if unauthorized and unintended information transfer via shared system resources is prevented.</i>	
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system security plan; system design documentation; system</p>	

	<p>configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer].</p> <p><b>Test:</b> [SELECT FROM: Separation of user functionality from system management functionality].</p>
--	--

<b>3.13.5</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</p>				
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p><i>Determine if:</i></p>				
	<table border="1" style="width: 100%;"> <tr> <td style="background-color: #002060; color: white; width: 15%; text-align: center;"><b>3.13.5[a]</b></td> <td><i>publicly accessible system components are identified.</i></td> </tr> <tr> <td style="background-color: #002060; color: white; text-align: center;"><b>3.13.5[b]</b></td> <td><i>subnetworks for publicly accessible system components are physically or logically separated from internal networks.</i></td> </tr> </table>	<b>3.13.5[a]</b>	<i>publicly accessible system components are identified.</i>	<b>3.13.5[b]</b>	<i>subnetworks for publicly accessible system components are physically or logically separated from internal networks.</i>
<b>3.13.5[a]</b>	<i>publicly accessible system components are identified.</i>				
<b>3.13.5[b]</b>	<i>subnetworks for publicly accessible system components are physically or logically separated from internal networks.</i>				
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing boundary protection capability].</p>				

<b>3.13.6</b>	<p><b>SECURITY REQUIREMENT</b></p> <p>Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).</p>				
	<p><b>ASSESSMENT OBJECTIVE</b></p> <p><i>Determine if:</i></p>				
	<table border="1" style="width: 100%;"> <tr> <td style="background-color: #002060; color: white; width: 15%; text-align: center;"><b>3.13.6[a]</b></td> <td><i>network communications traffic is denied by default.</i></td> </tr> <tr> <td style="background-color: #002060; color: white; text-align: center;"><b>3.13.6[b]</b></td> <td><i>network communications traffic is allowed by exception.</i></td> </tr> </table>	<b>3.13.6[a]</b>	<i>network communications traffic is denied by default.</i>	<b>3.13.6[b]</b>	<i>network communications traffic is allowed by exception.</i>
<b>3.13.6[a]</b>	<i>network communications traffic is denied by default.</i>				
<b>3.13.6[b]</b>	<i>network communications traffic is allowed by exception.</i>				
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms implementing traffic management at managed interfaces].</p>				

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



<b>3.13.7</b>	<b>SECURITY REQUIREMENT</b> Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. <b>Test:</b> [SELECT FROM: Mechanisms implementing boundary protection capability; mechanisms supporting or restricting non-remote connections].

<b>3.13.8</b>	<b>SECURITY REQUIREMENT</b> Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.13.8[a]</b>   <i>cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.</i>
	<b>3.13.8[b]</b>   <i>alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.</i>
	<b>3.13.8[c]</b>   <i>either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer]. <b>Test:</b> [SELECT FROM: Cryptographic mechanisms or mechanisms supporting or implementing transmission confidentiality; organizational processes for defining and implementing alternative physical safeguards].

<b>3.13.9</b>	<b>SECURITY REQUIREMENT</b>	
	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.13.9[a]</b>	<i>a period of inactivity to terminate network connections associated with communications sessions is defined.</i>
	<b>3.13.9[b]</b>	<i>network connections associated with communications sessions are terminated at the end of the sessions.</i>
	<b>3.13.9[c]</b>	<i>network connections associated with communications sessions are terminated after the defined period of inactivity.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing network disconnect; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer].	
	<b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing network disconnect capability].	

<b>3.13.10</b>	<b>SECURITY REQUIREMENT</b>	
	Establish and manage cryptographic keys for cryptography employed in organizational systems.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.13.10[a]</b>	<i>cryptographic keys are established whenever cryptography is employed.</i>
	<b>3.13.10[b]</b>	<i>cryptographic keys are managed whenever cryptography is employed.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment and management; system security plan; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].	
	<b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for cryptographic key establishment and management].	
	<b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing cryptographic key establishment and management].	

<b>3.13.11</b>	<b>SECURITY REQUIREMENT</b>	
	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.</i>	
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	

	<p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing cryptographic protection; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for cryptographic protection].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing cryptographic protection].</p>
--	--

<b>3.13.12</b>	<b>SECURITY REQUIREMENT</b>	
Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.		
<b>ASSESSMENT OBJECTIVE</b>		
<i>Determine if:</i>		
<b>3.13.12[a]</b>	<i>collaborative computing devices are identified.</i>	
<b>3.13.12[b]</b>	<i>collaborative computing devices provide indication to users of devices in use.</i>	
<b>3.13.12[c]</b>	<i>remote activation of collaborative computing devices is prohibited.</i>	
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>		
<p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for managing collaborative computing devices].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing management of remote activation of collaborative computing devices; mechanisms providing an indication of use of collaborative computing devices].</p>		

<b>3.13.13</b>	<b>SECURITY REQUIREMENT</b>	
Control and monitor the use of mobile code.		
<b>ASSESSMENT OBJECTIVE</b>		
<i>Determine if:</i>		
<b>3.13.13[a]</b>	<i>use of mobile code is controlled.</i>	
<b>3.13.13[b]</b>	<i>use of mobile code is monitored.</i>	
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>		
<p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; system audit logs and records; system security plan; list of acceptable mobile code and mobile code technologies; list of unacceptable mobile code and mobile technologies; authorization records; system monitoring records; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing mobile code].</p>		

	<p><b>Test:</b> [SELECT FROM: Organizational process for controlling, authorizing, monitoring, and restricting mobile code; mechanisms supporting or implementing the management of mobile code; mechanisms supporting or implementing the monitoring of mobile code].</p>
--	--

<b>3.13.14</b>	<p><b>SECURITY REQUIREMENT</b> Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.</p>				
	<p><b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i></p>				
	<table border="1"> <tr> <td style="background-color: #1a3d4d; color: white; text-align: center;"><b>3.13.14[a]</b></td> <td><i>use of Voice over Internet Protocol (VoIP) technologies is controlled.</i></td> </tr> <tr> <td style="background-color: #1a3d4d; color: white; text-align: center;"><b>3.13.14[b]</b></td> <td><i>use of Voice over Internet Protocol (VoIP) technologies is monitored.</i></td> </tr> </table>	<b>3.13.14[a]</b>	<i>use of Voice over Internet Protocol (VoIP) technologies is controlled.</i>	<b>3.13.14[b]</b>	<i>use of Voice over Internet Protocol (VoIP) technologies is monitored.</i>
<b>3.13.14[a]</b>	<i>use of Voice over Internet Protocol (VoIP) technologies is controlled.</i>				
<b>3.13.14[b]</b>	<i>use of Voice over Internet Protocol (VoIP) technologies is monitored.</i>				
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; VoIP implementation guidance; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; system monitoring records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing VoIP].</p> <p><b>Test:</b> [SELECT FROM: Organizational process for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP].</p>				

<b>3.13.15</b>	<p><b>SECURITY REQUIREMENT</b> Protect the authenticity of communications sessions.</p>
	<p><b>ASSESSMENT OBJECTIVE</b> <i>Determine if the authenticity of communications sessions is protected.</i></p>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b></p> <p><b>Examine:</b> [SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Mechanisms supporting or implementing session authenticity].</p>

<b>3.13.16</b>	<p><b>SECURITY REQUIREMENT</b> Protect the confidentiality of CUI at rest.</p>
	<p><b>ASSESSMENT OBJECTIVE</b> <i>Determine if the confidentiality of CUI at rest is protected.</i></p>

**POTENTIAL ASSESSMENT METHODS AND OBJECTS**

**Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information at rest; system security plan; system design documentation; list of information at rest requiring confidentiality protections; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; other relevant documents or records].

**Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer].

**Test:** [*SELECT FROM:* Mechanisms supporting or implementing confidentiality protections for information at rest].

### 3.14 SYSTEM AND INFORMATION INTEGRITY

<b>3.14.1</b>	<b>SECURITY REQUIREMENT</b> Identify, report, and correct system flaws in a timely manner.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.14.1[a]</b>   <i>the time within which to identify system flaws is specified.</i>
	<b>3.14.1[b]</b>   <i>system flaws are identified within the specified time frame.</i>
	<b>3.14.1[c]</b>   <i>the time within which to report system flaws is specified.</i>
	<b>3.14.1[d]</b>   <i>system flaws are reported within the specified time frame.</i>
	<b>3.14.1[e]</b>   <i>the time within which to correct system flaws is specified.</i>
	<b>3.14.1[f]</b>   <i>system flaws are corrected within the specified time frame.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility]. <b>Test:</b> [SELECT FROM: Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates].

<b>3.14.2</b>	<b>SECURITY REQUIREMENT</b> Provide protection from malicious code at designated locations within organizational systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
	<b>3.14.2[a]</b>   <i>designated locations for malicious code protection are identified.</i>
	<b>3.14.2[b]</b>   <i>protection from malicious code at designated locations is provided.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation; system audit logs and records; other relevant documents or records].

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

	<p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting or implementing malicious code scanning and subsequent actions].</p>
--	---

<b>3.14.3</b>	<b>SECURITY REQUIREMENT</b>
Monitor system security alerts and advisories and take action in response.	
<b>ASSESSMENT OBJECTIVE</b>	
Determine if:	
<b>3.14.3[a]</b>	<i>response actions to system security alerts and advisories are identified.</i>
<b>3.14.3[b]</b>	<i>system security alerts and advisories are monitored.</i>
<b>3.14.3[c]</b>	<i>actions in response to system security alerts and advisories are taken.</i>
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: System and information integrity policy; procedures addressing security alerts, advisories, and directives; system security plan; records of security alerts and advisories; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: Personnel with security alert and advisory responsibilities; personnel implementing, operating, maintaining, and using the system; personnel, organizational elements, and external organizations to whom alerts, advisories, and directives are to be disseminated; system or network administrators; personnel with information security responsibilities].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; mechanisms supporting or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives; mechanisms supporting or implementing security directives].</p>	

<b>3.14.4</b>	<b>SECURITY REQUIREMENT</b>
Update malicious code protection mechanisms when new releases are available.	
<b>ASSESSMENT OBJECTIVE</b>	
Determine if malicious code protection mechanisms are updated when new releases are available.	
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
<p><b>Examine:</b> [SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].</p>	

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

	<p><b>Test:</b> [SELECT FROM: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing malicious code protection mechanisms (including updates and configurations); mechanisms supporting or implementing malicious code scanning and subsequent actions].</p>
--	---

<b>3.14.5</b>	<b>SECURITY REQUIREMENT</b>	
	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.14.5[a]</b>	<i>the frequency for malicious code scans is defined.</i>
	<b>3.14.5[b]</b>	<i>malicious code scans are performed with the defined frequency.</i>
	<b>3.14.5[c]</b>	<i>real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing malicious code protection mechanisms (including updates and configurations); mechanisms supporting or implementing malicious code scanning and subsequent actions].</p>	

<b>3.14.6</b>	<b>SECURITY REQUIREMENT</b>	
	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.14.6[a]</b>	<i>the system is monitored to detect attacks and indicators of potential attacks.</i>
	<b>3.14.6[b]</b>	<i>inbound communications traffic is monitored to detect attacks and indicators of potential attacks.</i>
	<b>3.14.6[c]</b>	<i>outbound communications traffic is monitored to detect attacks and indicators of potential attacks.</i>



<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	<p><b>Examine:</b> [SELECT FROM: System and information integrity policy; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram or layout; system security plan; system monitoring tools and techniques documentation; system design documentation; locations within system where monitoring devices are deployed; system protocols; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility monitoring the system; personnel with responsibility for the intrusion detection system].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing intrusion detection capability and system monitoring; mechanisms supporting or implementing system monitoring capability; organizational processes for intrusion detection and system monitoring; mechanisms supporting or implementing the monitoring of inbound and outbound communications traffic].</p>
---	---

<b>3.14.7</b>	<b>SECURITY REQUIREMENT</b>	
	Identify unauthorized use of organizational systems.	
	<b>ASSESSMENT OBJECTIVE</b>	
	<i>Determine if:</i>	
	<b>3.14.7[a]</b>	<i>authorized use of the system is defined.</i>
	<b>3.14.7[b]</b>	<i>unauthorized use of the system is identified.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b>	
	<p><b>Examine:</b> [SELECT FROM: Continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram/layout; system security plan; system design documentation; system monitoring tools and techniques documentation; locations within system where monitoring devices are deployed; system configuration settings and associated documentation; other relevant documents or records].</p> <p><b>Interview:</b> [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for monitoring the system].</p> <p><b>Test:</b> [SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing system monitoring capability].</p>	

## APPENDIX A

## REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES<sup>9</sup>

## LEGISLATION, EXECUTIVE ORDERS, AND REGULATIONS

1. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014.  
<https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf>
2. Executive Order 13526, *Classified National Security Information*, December 2009.  
<https://www.archives.gov/isoo/policy-documents/cnsi-eo.html>
3. Executive Order 13556, *Controlled Unclassified Information*, November 2010.  
<https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf>
4. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.  
<https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
5. 32 CFR Part 2002, *Controlled Unclassified Information*, September 2016.  
<https://www.gpo.gov/fdsys/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf>

## STANDARDS, GUIDELINES, INTERAGENCY REPORTS, AND INSTRUCTIONS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.  
<https://doi.org/10.6028/NIST.FIPS.199>
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.  
<https://doi.org/10.6028/NIST.FIPS.200>
3. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.  
<https://doi.org/10.6028/NIST.SP.800-39>
4. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.  
<https://doi.org/10.6028/NIST.SP.800-53r4>
5. National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014.  
<https://doi.org/10.6028/NIST.SP.800-53Ar4>

<sup>9</sup> References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

6. National Institute of Standards and Technology Special Publication 171, Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016.  
<https://doi.org/10.6028/NIST.SP.800-171r1>
7. National Institute of Standards and Technology Special Publication 128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.  
<https://doi.org/10.6028/NIST.SP.800-128>
8. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, September 2013.
9. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, September 2013.
10. Committee on National Security Systems Instruction 4009, *National Information Assurance Glossary*, April 2015.  
<https://www.cnss.gov>
11. National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017.  
<https://doi.org/10.6028/NIST.IR.8062>

#### OTHER RESOURCES

1. National Archives and Records Administration, *Controlled Unclassified Information Registry*.  
<https://www.archives.gov/cui/registry/category-list>
2. National Institute of Standards and Technology Handbook 162, *NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, November 2017.  
<https://doi.org/10.6028/NIST.HB.162>

## APPENDIX B

## GLOSSARY

## COMMON TERMS AND DEFINITIONS

**A**ppendix B provides definitions for security terminology used within Special Publication 800-171. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in [CNSS Instruction 4009](#), *National Information Assurance Glossary*.

<b>agency</b>	See <i>executive agency</i> .
<b>assessment</b>	See <i>Security Control Assessment</i> .
<b>assessor</b>	See <i>Security Control Assessor</i> .
<b>audit log</b>	A chronological record of system activities, including records of system accesses and operations performed in a given period.
<b>audit record</b>	An individual entry in an audit log related to an audited event.
<b>authentication</b> [FIPS 200, Adapted]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
<b>availability</b> [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
<b>baseline configuration</b>	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
<b>blacklisting</b>	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
<b>confidentiality</b> [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
<b>configuration management</b>	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
<b>configuration settings</b>	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
<b>controlled area</b>	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

<p><b>controlled unclassified information</b> [E.O. 13556]</p>	<p>Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, <i>Classified National Security Information</i>, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.</p>
<p><b>CUI categories or subcategories</b> [Title 32 CFR, Part 2002]</p>	<p>Those types of information for which laws, regulations, or governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.</p>
<p><b>CUI Executive Agent</b> [Title 32 CFR, Part 2002]</p>	<p>The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).</p>
<p><b>CUI program</b> [Title 32 CFR, Part 2002]</p>	<p>The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.</p>
<p><b>CUI registry</b> [Title 32 CFR, Part 2002]</p>	<p>The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.</p>
<p><b>environment of operation</b> [NIST SP 800-37, Adapted]</p>	<p>The physical surroundings in which a system processes, stores, and transmits information.</p>
<p><b>executive agency</b> [41 U.S.C., Sec. 403]</p>	<p>An executive department specified in 5 U.S.C., Sec. 105; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.</p>
<p><b>external system (or component)</b></p>	<p>A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.</p>
<p><b>external system service</b></p>	<p>A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.</p>

<b>external system service provider</b>	A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
<b>external network</b>	A network not controlled by the organization.
<b>federal agency</b>	See <i>executive agency</i> .
<b>federal information system</b> [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. See <i>on behalf of (an agency)</i> for additional information.
<b>FIPS-validated cryptography</b>	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See <i>NSA-Approved Cryptography</i> .
<b>firmware</b>	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
<b>hardware</b>	The physical components of a system. See <i>Software</i> and <i>Firmware</i> .
<b>identifier</b>	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.
<b>impact</b>	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.
<b>impact value</b>	The assessed potential impact resulting from a compromise of the confidentiality of information (e.g., CUI) expressed as a value of low, moderate, or high.
<b>incident</b> [FIPS 200, Adapted]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
<b>information</b>	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

<b>information flow control</b>	Procedure to ensure that information transfers within a system are not made in violation of the security policy.
<b>information resources</b> [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
<b>information security</b> [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
<b>information system</b> [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
<b>information technology</b> [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term <i>information technology</i> includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
<b>insider threat</b>	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.
<b>integrity</b> [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
<b>internal network</b>	A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
<b>least privilege</b>	The principle that a system security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

<b>local access</b>	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
<b>malicious code</b>	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
<b>media</b> [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.
<b>mobile code</b>	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.
<b>mobile device</b>	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.
<b>multifactor authentication</b>	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See also <i>Authenticator</i> .
<b>nonfederal organization</b>	An entity that owns, operates, or maintains a nonfederal system.
<b>nonfederal system</b>	A system that does not meet the criteria for a federal system.
<b>network</b>	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
<b>network access</b>	Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
<b>nonlocal maintenance</b>	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.



<b>on behalf of (an agency)</b> [32 CFR Part 2002]	A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government.
<b>organization</b> [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure.
<b>portable storage device</b>	A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).
<b>potential impact</b> [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a <i>limited</i> adverse effect (FIPS Publication 199 low); (ii) a <i>serious</i> adverse effect (FIPS Publication 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
<b>privileged account</b>	A system account with authorizations of a privileged user.
<b>privileged user</b>	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
<b>records</b>	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
<b>remote access</b>	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
<b>remote maintenance</b>	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
<b>replay resistance</b>	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

<b>risk</b> [FIPS 200, Adapted]	<p>A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.</p> <p>System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation.</p>
<b>risk assessment</b>	<p>The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.</p> <p>Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.</p>
<b>sanitization</b>	<p>Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.</p> <p>Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.</p>
<b>security</b>	<p>A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that form part of the enterprise's risk management approach.</p>
<b>security assessment</b>	<p>See <i>Security Control Assessment</i>.</p>
<b>security control</b> [FIPS 199, Adapted]	<p>A safeguard or countermeasure prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.</p>
<b>security control assessment</b> [CNSSI 4009, Adapted]	<p>The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for a system or organization.</p>
<b>security functionality</b>	<p>The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational systems or the environments in which those systems operate.</p>
<b>security functions</b>	<p>The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.</p>

<b>security relevance</b>	Functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.
<b>situational awareness</b> [CNSSI 4009]	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.
<b>split tunneling</b>	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.
<b>supplemental guidance</b>	Statements used to provide additional explanatory information for security controls or security control enhancements.
<b>system</b>	See <i>Information System</i> .
<b>system component</b> [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.
<b>system security plan</b>	A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. The system security plan describes the system boundary; the environment in which the system operates; the relationships with or connections to other systems; and how the security requirements are implemented.
<b>system service</b>	A capability provided by a system that facilitates information processing, storage, or transmission.
<b>threat</b> [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
<b>user</b> [CNSSI 4009, Adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
<b>whitelisting</b>	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.
<b>wireless technology</b>	Technology that permits the transfer of information between separated points without physical connection.

## APPENDIX C

### ACRONYMS

#### COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
ITL	Information Technology Laboratory
NARA	National Archives and Records Administration
NFO	Nonfederal Organization
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
SSP	System Security Plan

## APPENDIX D

### ASSESSMENT METHODS

#### ASSESSMENT METHOD DEFINITIONS, APPLICABLE OBJECTS, AND ATTRIBUTES

This appendix defines three assessment methods that can be used to assess the CUI security requirements in [NIST Special Publication 800-171](#): *examine*, *interview*, and *test*. Included in the definition of each assessment method are types of objects to which the method can be applied. The application of each method is described in terms of the attributes of *depth* and *coverage*, progressing from *basic* to *focused* to *comprehensive*. The attribute values correlate to the assurance requirements specified by the organization.

The depth attribute addresses the rigor and level of detail of the assessment. For the depth attribute, the *focused* attribute value includes and builds upon the assessment rigor and level of detail defined for the *basic* attribute value; the *comprehensive* attribute value includes and builds upon the assessment rigor and level of detail defined for the *focused* attribute value.

The coverage attribute addresses the scope or breadth of the assessment. For the coverage attribute, the *focused* attribute value includes and builds upon the number and type of assessment objects defined for the *basic* attribute value; the *comprehensive* attribute value includes and builds upon the number and type of assessment objects defined for the *focused* attribute value.

Tables D-1 through D-3 provide complete descriptions of the *examine*, *interview*, and *test* assessment methods. The use of **bolded text** in the assessment method description indicates the content that was added to and appears for the first time, in the description indicating greater rigor and level of detail for the attribute value.

**TABLE D-1: EXAMINE ASSESSMENT METHOD**

<b>Method</b>	<b>EXAMINE</b> The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.	
<b>Objects</b>	<b>Specifications</b>	Examples: policies, plans, procedures, system requirements, designs.
	<b>Mechanisms</b>	Examples: functionality implemented in hardware, software, firmware.
	<b>Activities</b>	Examples: system operations, administration, management, exercises.
<b>Attributes</b>	<b>Depth</b>	Addresses the rigor of and level of detail in the <i>examination</i> process.
	<b>Basic</b>	Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation. Examples include: functional-level descriptions for mechanisms; high-level process descriptions for activities; and documents for specifications. Basic examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
	<b>Focused</b>	Examination that consists of high-level reviews, checks, observations, or inspections <b>and more in-depth studies and analyses</b> of the assessment object. This type of examination is conducted using a <b>substantial</b> body of evidence or documentation. Examples include: functional-level descriptions <b>and where appropriate and available, high-level design information</b> for mechanisms; high-level process descriptions <b>and implementation procedures</b> for activities; and documents <b>and related documents</b> for specifications. <b>Focused</b> examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors <b>and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.</b>
	<b>Comprehensive</b>	Examination that consists of high-level reviews, checks, observations, or inspections and more in-depth, <b>detailed, and thorough</b> studies and analyses of the assessment object. This type of examination is conducted using an <b>extensive</b> body of evidence or documentation. Examples include: functional-level descriptions and where appropriate and available, high-level design information, <b>low-level design information, and implementation information</b> for mechanisms; high-level process descriptions and <b>detailed</b> implementation procedures for activities; and documents and related documents for specifications. <sup>10</sup> <b>Comprehensive</b> examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are <b>further</b> increased grounds for confidence that the safeguards are implemented correctly and operating as intended <b>on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.</b>

<sup>10</sup> While additional documentation is likely for mechanisms when moving from basic to focused to comprehensive examinations, the documentation associated with specifications and activities may be the same or similar for focused and comprehensive examinations, with the rigor of the examinations of these documents being increased at the comprehensive level.

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

<b>Coverage</b>	Addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined; the number of objects to be examined by type; and specific objects to be examined. <sup>11</sup>	
	<b>Basic</b>	Examination that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.
	<b>Focused</b>	Examination that uses a representative sample of assessment objects (by type and number within type) <b>and other specific assessment objects deemed particularly important to achieving the assessment objective</b> to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors <b>and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.</b>
	<b>Comprehensive</b>	Examination that uses a <b>sufficiently large</b> sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors and whether there are <b>further</b> increased grounds for confidence that the safeguards are implemented correctly and operating as intended <b>on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.</b>
<p><b>DISCUSSION</b></p> <p>Typical assessor actions may include, for example: reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations; reviewing training records; reviewing audit records; observing incident response activities; studying technical manuals and user/administrator guides; checking, studying, or observing the operation of an information technology mechanism in the system hardware or software; or checking, studying, or observing physical security measures related to the operation of a system.</p>		

<sup>11</sup> The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization’s overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific objects to be examined for the attribute value described.

**TABLE D-2: INTERVIEW ASSESSMENT METHOD**

<b>Method</b>	<b>INTERVIEW</b> The process of conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.	
<b>Objects</b>	<b>Individuals or Groups</b>	Examples: Personnel with risk assessment responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities.
<b>Attributes</b>	<b>Depth</b>	Addresses the rigor of and level of detail in the <i>interview</i> process.
	<b>Basic</b>	Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Basic interviews provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
	<b>Focused</b>	Interview that consists of broad-based, high-level discussions <b>and more in-depth discussions in specific areas</b> with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions <b>and more in-depth questions in specific areas where responses indicate a need for more in-depth investigation. Focused</b> interviews provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors <b>and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.</b>
	<b>Comprehensive</b>	Interview that consists of broad-based, high-level discussions and more in-depth, <b>probing</b> discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in-depth, <b>probing</b> questions in specific areas where responses indicate a need for more in-depth investigation. <b>Comprehensive</b> interviews provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are <b>further</b> increased grounds for confidence that the safeguards are implemented correctly and operating as intended <b>on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.</b>
	<b>Coverage</b>	Addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed by role and responsibility; the number of individuals to be interviewed by type; and specific individuals to be interviewed. <sup>12</sup>
	<b>Basic</b>	Interview that uses a representative sample of individuals in organizational roles to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.

<sup>12</sup> The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization’s overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific individuals to be interviewed for the attribute value described.

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



		<i>Focused</i>	Interview that uses a representative sample of individuals in organizational roles <b>and other specific individuals deemed particularly important to achieving the assessment objective</b> to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors <b>and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.</b>
		<i>Comprehensive</i>	Interview that uses a <b>sufficiently large</b> sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors and whether there are <b>further</b> increased grounds for confidence that the safeguards are implemented correctly and operating as intended <b>on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.</b>
	<p><b>DISCUSSION</b></p> <p>Typical assessor actions may include, for example, interviewing chief executive officers, chief information officers, senior information security officers, information owners, system and mission owners, system security officers, system security managers, personnel officers, human resource managers, network and system administrators, facilities managers, training officers, physical security officers, system operators, site managers, and users.</p>		

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

**TABLE D-3: TEST ASSESSMENT METHOD**

<b>Method</b>	<b>TEST</b> The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. <sup>13</sup>	
<b>Objects</b>	<b>Mechanisms</b>	Examples: hardware, software, firmware.
	<b>Activities</b>	Examples: system operations, administration, management; exercises.
<b>Attributes</b>	<b>Depth</b>	Addresses the types of testing to be conducted.
		<b>Basic</b> Test methodology (also known as <i>black box</i> testing) that assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Basic testing provides a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
		<b>Focused</b> Test methodology (also known as <i>gray box</i> testing) that assumes <b>some</b> knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification <b>and limited system architectural information (e.g., high-level design)</b> for mechanisms and a high-level process description <b>and high-level description of integration into the operational environment</b> for activities. Focused testing provides a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors <b>and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.</b>
	<b>Comprehensive</b> Test methodology (also known as <i>white box</i> testing) that assumes <b>explicit and substantial</b> knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, <b>extensive</b> system architectural information (e.g., high-level design, <b>low-level design</b> ) <b>and implementation representation (e.g., source code, schematics)</b> for mechanisms and a high-level process description and <b>detailed</b> description of integration into the operational environment for activities. Comprehensive testing provides a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are <b>further</b> increased grounds for confidence that the safeguards are implemented correctly and operating as intended <b>on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.</b>	
	<b>Coverage</b>	Addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested; the number of objects to be tested by type; and specific objects to be tested.

<sup>13</sup> Testing is typically used to determine if mechanisms or activities meet a set of predefined specifications. Testing can also be performed to determine characteristics of a security or privacy control that are not commonly associated with predefined specifications, with an example of such testing being penetration testing.

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

		<b>Basic</b>	Testing that uses a representative sample of assessment objects by type and number within type, to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.
		<b>Focused</b>	Testing that uses a representative sample of assessment objects by type and number within type, <b>and other specific assessment objects deemed particularly important to achieving the assessment objective</b> to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors <b>and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.</b>
		<b>Comprehensive</b>	Testing that uses a <b>sufficiently large</b> sample of assessment objects by type and number within type, and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors and whether there are <b>further</b> increased grounds for confidence that the safeguards are implemented correctly and operating as intended <b>on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.</b>
	<p><b>DISCUSSION</b></p> <p>Typical assessor actions may include, for example: testing access control, identification and authentication, and audit mechanisms; testing security configuration settings; testing physical access control devices; conducting penetration testing of key system components; testing system backup operations; testing incident response capability; and exercising vulnerability scanning capability.</p>		

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

**NIST Handbook 162**

**NIST MEP Cybersecurity  
Self-Assessment Handbook  
For Assessing NIST SP 800-171  
Security Requirements in Response to  
DFARS Cybersecurity Requirements**

Patricia Toth

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.HB.162>

**NIST**  
**National Institute of  
Standards and Technology**  
U.S. Department of Commerce

# NIST Handbook 162

## **NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements**

Patricia Toth  
*Programs and Partnerships Division  
Manufacturing Extension Partnership*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.HB.162>

November 2017



U.S. Department of Commerce  
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology  
*Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology*

## **Abstract**

The Handbook is intended to be a guide to assist U.S. manufacturers who supply products within supply chains for the DOD and who must ensure adequate security by implementing NIST SP 800-171 as part of the process for ensuring compliance with DFARS clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting,” available at <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012>.

## **Key words**

assessment; compliance; Controlled Unclassified Information; CUI; cybersecurity; DFARS; DOD supply chain; information security; manufacturing; MEP; small manufacturer; self-assessment; SP 800-171.

## Table of Contents

<b>Disclaimer .....</b>	<b>viii</b>
<b>Acknowledgements .....</b>	<b>viii</b>
<b>About NIST MEP and the MEP National Network™ .....</b>	<b>viii</b>
<b>Introduction.....</b>	<b>1</b>
Role of NIST in SP 800-171 .....	1
What is NIST SP 800-171 and how does a manufacturer implement it?.....	2
<b>Using this Handbook to Conduct an Assessment.....</b>	<b>4</b>
Preparation .....	4
Assessment Results .....	6
<b>Self-Assessment Handbook .....</b>	<b>7</b>
Access Control: SP 800-171 Security Family 3.1.....	7
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).....	8
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute. ....	9
3.1.3 Control the flow of CUI in accordance with approved authorizations. ....	10
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.....	11
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.....	12
3.1.6 Use non-privileged accounts or roles when accessing non-security functions. ...	13
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.....	14
3.1.8 Limit unsuccessful logon attempts. ....	15
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.....	16
3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity. ....	17
3.1.11 Terminate (automatically) a user session after a defined condition.....	18
3.1.12 Monitor and control remote access sessions. ....	19
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. ....	20
3.1.14 Route remote access via managed access control points.....	21
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.....	22
3.1.16 Authorize wireless access prior to allowing such connections. ....	23

- 3.1.17 Protect wireless access using authentication and encryption..... 24
- 3.1.18 Control connection of mobile devices..... 25
- 3.1.19 Encrypt CUI on mobile devices. .... 26
- 3.1.20 Verify and control/limit connections to and use of external information systems.27
- 3.1.21 Limit use of organization portable storage devices on external information systems. 28
- 3.1.22 Control CUI posted or processed on publicly accessible information systems. ... 29
- Awareness and Training: SP 800-171 Security Family 3.2 ..... 30
  - 3.2.1 Ensure that managers, systems administrators, and users of organization information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organization information systems. .... 31
  - 3.2.2 Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities..... 32
  - 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. .... 33
- Audit and Accountability: SP 800-171 Security Family 3.3..... 34
  - 3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. .... 35
  - 3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions..... 36
  - 3.3.3 Review and update audited events..... 37
  - 3.3.4 Alert in the event of an audit process failure..... 38
  - 3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. .... 39
  - 3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting..... 40
  - 3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records..... 41
  - 3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion. .... 42
  - 3.3.9 Limit management of audit functionality to a subset of privileged users..... 43
- Configuration Management: SP 800-171 Security Family 3.4 ..... 44
  - 3.4.1 Establish and maintain baseline configurations and inventories of organization information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. .... 45



3.4.2	Establish and enforce security configuration settings for information technology products employed in organization information systems. ....	47
3.4.3	Track, review, approve/disapprove, and audit changes to information systems... ..	48
3.4.4	Analyze the security impact of changes prior to implementation. ....	49
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.....	50
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.....	51
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. ....	52
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting policy to allow the execution of authorized software.....	53
3.4.9	Control and monitor user-installed software.....	55
	Identification and Authentication: SP 800-171 Security Family 3.5 .....	56
3.5.1	Identify information system users, processes acting on behalf of users, or devices.....	57
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to company information systems.....	58
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.....	59
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.....	61
3.5.5	Prevent reuse of identifiers for a defined period.....	62
3.5.6	Disable identifiers after a defined period of inactivity.....	63
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created. ....	64
3.5.8	Prohibit password reuse for a specified number of generations. ....	65
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.....	66
3.5.10	Store and transmit only encrypted representation of passwords. ....	67
3.5.11	Obscure feedback of authentication information. ....	68
	Incident Response: SP 800-171 Security Family 3.6.....	69
3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.....	70
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.....	71
3.6.3	Test the organization incident response capability. ....	73

- Maintenance: SP 800-171 Security Family 3.7..... 74
  - 3.7.1 Perform maintenance on organization information systems. .... 75
  - 3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. .... 76
  - 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. .... 77
  - 3.7.4 Check media containing diagnostics and test programs for malicious code before the media are used in the information system. .... 78
  - 3.7.5 Require multifactor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete..... 79
  - 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. .... 80
- Media Protection: SP 800-171 Security Family 3.8..... 81
  - 3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital. .... 82
  - 3.8.2 Limit access to CUI on information system media to authorized users. .... 83
  - 3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse. .... 84
  - 3.8.4 Mark media with necessary CUI markings and distribution limitations. .... 85
  - 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas..... 86
  - 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 87
  - 3.8.7 Control the use of removable media on information system components..... 88
  - 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 89
  - 3.8.9 Protect the confidentiality of backup CUI at storage locations. .... 90
- Personnel Security: SP 800-171 Security Family 3.9 ..... 91
  - 3.9.1 Screen individuals prior to authorizing access to information systems containing CUI. 92
  - 3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers..... 93
- Physical Protection: SP 800-171 Security Family 3.10 ..... 94
  - 3.10.1 Limit physical access to company information systems, equipment, and the respective operating environments to authorized individuals..... 95
  - 3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems. .... 96

3.10.3 Escort visitors and monitor visitor activity. ....	97
3.10.4 Maintain audit logs of physical access. ....	98
3.10.5 Control and manage physical access devices. ....	99
3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). 100	
Risk Assessment: SP 800-171 Security Family 3.11 .....	101
3.11.1 Periodically assess the risk to company operations (including mission, functions, image, or reputation), company assets, and individuals, resulting from the operation of company information systems and the associated processing, storage, or transmission of CUI. 102	
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.....	103
3.11.3 Remediate vulnerabilities in accordance with assessments of risk. ....	105
Security Assessment: SP 800-171 Security Family 3.12 .....	106
3.12.1 Periodically assess the security controls in company information systems to determine if the controls are effective in their application. ....	107
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company information systems. ....	109
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. ....	110
3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. ....	112
Systems and Communications Protection: SP 800-171 Security Family 3.13 .....	114
3.13.1 Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems. ....	115
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within company information systems. ....	116
3.13.3 Separate user functionality from information system management functionality. ....	118
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. ....	119
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.....	120
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).....	121

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.....	122
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. ....	123
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.....	125
3.13.10 Establish and manage cryptographic keys for cryptography employed in the organization systems.....	126
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	127
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.....	128
3.13.13 Control and monitor the use of mobile code.....	129
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	130
3.13.15 Protect the authenticity of communications sessions. ....	131
3.13.16 Protect the confidentiality of CUI at rest. ....	132
System and Information Integrity: SP 800-171 Security Family 3.14.....	133
3.14.1 Identify, report, and correct information and information system flaws in a timely manner. ....	134
3.14.2 Provide protection from malicious code at appropriate locations within organization information systems. ....	136
3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response. ....	138
3.14.4 Update malicious code protection mechanisms when new releases are available.	140
3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.....	142
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. ....	143
3.14.7 Identify unauthorized use of the information system.....	144
<b>Glossary .....</b>	<b>145</b>
<b>Appendix A: Useful Plans, Policies and Procedures.....</b>	<b>157</b>

## Disclaimer

The contents of this Handbook are offered as guidance only. NIST and NIST MEP do not make any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this Handbook, or that the use of any information, methods, or processes described in this Handbook may not infringe on privately owned rights; or assume any liabilities with respect to the use of, or for damages resulting from the use of, any information, method, or process described in this Handbook. The Handbook does not reflect official views or policy of NIST. Mention of trade names or commercial products does not constitute endorsement by or recommendation of use by NIST.

This Handbook has been produced by NIST MEP technical staff and has been reviewed by technical staff within the NIST Information Technology Laboratory. The Handbook is intended to be a guide to assist U.S. manufacturers who supply products within supply chains for the Department of Defense (DOD) and who must ensure adequate security by implementing NIST SP 800-171 as part of the process for ensuring compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting,” available at <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252204-7012>.

This Handbook includes mention of official DOD policies and regulations that are part of the aforementioned DFARS clause. Such mention is public domain information and does not constitute any policy statements or regulatory enforcement by NIST. NIST is a non-regulatory agency of the U.S. Department of Commerce; as such, NIST makes no claims that use of this Handbook will satisfy the regulatory requirements of DOD in conjunction with DFARS. Compliance with the DFARS can only be satisfied through approval by the DOD in conjunction with official DFARS requirements. All matters relating to the DFARS should be directed to the DOD in conjunction with the requirements of DFARS clause 252.204-7012. Additional information about the DFARS can be obtained at [http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation\\_FAQ.pdf](http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf).

## Acknowledgements

The author gratefully acknowledges and appreciates the thoughtful comments from NIST MEP staff members David Stieren, Brian Lagas, Marlon Walker, and Kathleen Martin, which greatly improved the overall quality and usefulness of this Handbook. Additionally, Ron Ross and Kelley Dempsey from the NIST Information Technology Laboratory’s Computer Security Division provided technical guidance on the implementation of SP 800-171. Useful feedback was also received from several staff members within the DOD Office of the Chief Information Officer to ensure consistency with DFARS provisions.

## About NIST MEP and the MEP National Network™

Since 1988, the National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP) has been committed to strengthening U.S. manufacturing. The MEP National Network comprises 51 MEP Centers located in all 50 states and Puerto Rico, and 1,300 trusted advisors and experts at nearly 600 MEP service locations, providing any U.S. manufacturer with access to resources they need to succeed. In 2016, the MEP National Network connected with

25,445 manufacturers, leading to \$9.3 billion in sales, \$1.4 billion in cost savings, \$3.5 billion in new client investments, and helping to create and retain more than 86,602 U.S. manufacturing jobs.

### Supply Chain, Defense, and Cybersecurity Focus

MEP provides hands-on technical and business assistance supporting the development and competitiveness of manufacturing supply chains, including those that serve the needs of our Nation's defense industries. MEP supports U.S. manufacturers with many different aspects of supply chain management and development, including implementing strategies within the walls of a company, to engaging with suppliers and customers around the Nation and the world. Recently, MEP has been active in providing awareness and assistance to help U.S. manufacturers protect their information assets from the risks of cyberattacks. MEP serves as a national resource to help U.S. manufacturers, who supply to the DOD, implement adequate security to safeguard covered defense information that they store, process, or transmit.

Since 2013, MEP Centers have completed 2,567 projects and worked with 1,658 companies that are prime suppliers to the DOD. MEP also works with large OEM-type suppliers and their supply chains to the DOD. From 2013 to 2016, MEP worked with 706 companies that have defense industry NAICS classifications.

For additional information, visit the NIST MEP webpage at <https://www.nist.gov/mep>.

## Introduction

This Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in response to DFARS Cybersecurity Requirements provides guidance on implementing NIST SP 800-171 in response to the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting.”

This Handbook provides a step-by-step guide to assessing a small manufacturer’s information systems against the security requirements in NIST SP 800-171 rev 1, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-171r1.pdf>.

This Handbook may also be useful for other communities interested in applying the NIST SP 800-171 security requirements, including those seeking to comply with the CUI Federal Acquisition Regulation (FAR) clause.

## Role of NIST in SP 800-171

Executive Order 13556, Controlled Unclassified Information, November 4, 2010, establishes that the Controlled Unclassified Information (CUI) Executive Agent, designated as the National Archives and Records Administration (NARA), shall develop and issue such directives as are necessary to implement the CUI Program. Consistent with this tasking and with the CUI Program’s mission to establish uniform policies and practices across the federal government, NARA issued a final federal regulation in 2016 that established the required controls and markings for CUI governmentwide. This federal regulation binds agencies throughout the executive branch to uniformly apply the standard safeguards, markings, dissemination, and decontrol requirements established by the CUI Program.

In addition to defining safeguarding requirements for CUI within the federal government, NARA took to alleviate the potential impact of such requirements on nonfederal organizations by jointly developing with NIST and DOD, NIST Special Publication 800-171, and defining security requirements for protecting CUI in nonfederal systems and organizations. This approach was intended to help nonfederal entities, including contractors, to comply with the security requirements using the systems and practices they already have in place, rather than trying to use government-specific approaches. It also provides a standardized and uniform set of requirements for all CUI security needs, tailored to nonfederal systems, allowing nonfederal organizations to be in compliance with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI. Finally, NARA, in its capacity as the CUI Executive Agent, sponsored in 2017, a single Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the federal CUI regulation and Special Publication 800-171 to contractors. This will further promote standardization to benefit a substantial number of nonfederal organizations that are attempting to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from federal agencies for the same information gives rise to confusion and inefficiencies. The CUI FAR clause will also address verification and compliance requirements for the security requirements in NIST Special Publication 800-171. Until the formal process of establishing such a FAR clause takes place, the requirements in NIST Special Publication 800-171 may be

referenced in federal contracts consistent with federal law and regulatory requirements. If necessary, Special Publication 800-171 will be updated to remain consistent with the federal CUI regulation and the FAR clause.

### **What is NIST SP 800-171 and how does a manufacturer implement it?**

NIST Special Publication 800-171 was developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. 3541 et seq., Public Law (P.L.) 113-283. The publication is entitled “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” NIST SP 800-171 Revision 1, available at

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf>.

NIST SP 800-171 provides federal agencies with recommended requirements for protecting the confidentiality of controlled unclassified information (CUI):

1. when the CUI is resident in nonfederal information systems and organizations;
2. when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
3. where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

NIST SP 800-171 requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. A nonfederal information system is a system that does not meet the criteria for a federal system. A federal system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This includes the DOD and is resident within DFARS clauses that apply to defense contracts.

For ease of use, the NIST SP 800-171 security requirements are organized into 14 families. This Self-Assessment Handbook is organized based on these 14 families.

For each family, a brief overview is provided. Table 1 below lists the security requirement families addressed in this Handbook.



FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	Systems and Communications Protection
Maintenance	System and Information Integrity

Table 1. NIST SP 800-171 Security Requirement Families

The security requirement with the original numbering scheme from 800-171 is listed throughout this Handbook.

NIST SP 800-171 assumes that small manufacturers currently have IT infrastructures in place, and it is not necessary to develop or acquire new systems to handle CUI. Most small manufacturers have security measures to protect their information which may also satisfy the 800-171 security requirements. A variety of potential security solutions can be implemented to satisfy the security requirements. There is no single security solution, each small manufacturer will need to understand their operating environment and apply the security requirements to meet their situation. Small manufacturers may not have the necessary organizational structure or resources to satisfy every security requirement. It is perfectly acceptable to implement alternative, but equally effective, security measures to satisfy a security requirement.

## Using this Handbook to Conduct an Assessment

### Preparation

This Handbook is intended for use by a small manufacturer. It is expected that the business owner, chief operating officer, IT manager, security manager, and plant manager(s) will work together to assess the security of the system(s) that process, store, or transmit CUI.

Conducting security control assessments can be challenging, and resource-intensive. Successful assessments require cooperation throughout the company. Establishing expectations before, during, and after an assessment is important to achieve an acceptable outcome. Thorough preparation is an important aspect of conducting effective security control assessments.

Preparatory activities address issues relating to the cost, schedule, and performance of the assessment. Preparing for a security control assessment includes:

- ensuring that security policies are in place and understood by company employees. A list of plans and polices companies should have in place is included in Appendix A;
- establishing the objective and scope of assessments;
- notifying key employees of assessment activities and allocating resources to carry out the assessments;
- establishing communication channels among employees having an interest in the assessments;
- establishing time frames for completing the assessments;
- selecting the assessors/assessment teams that will be responsible for conducting the assessments; and
- collecting materials to provide to the assessors/assessment teams. (This may include policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous assessment results, and legal requirements.)

Security control assessors/assessment teams begin the assessment by:

- gaining an understanding of the company's operations (including mission, functions, and business processes) and how the information system supports those organizational operations;
- obtaining an understanding of the structure of the information system (i.e., system architecture) being assessed;
- identifying company personnel responsible for the development and implementation of the security requirements;
- meeting with company personnel to ensure understanding for assessment objectives,

rigor, and scope of the assessment;

- obtaining materials needed for the assessment (e.g., policies, procedures, plans, specifications, designs, records, administrator and operator manuals, information system documentation, interconnection agreements, previous assessment results);
- establishing company points of contact needed to carry out the assessments;
- obtaining previous assessment results that may be reused (e.g., audits, vulnerability scans, physical security inspections, prior security assessments, developmental testing and evaluation, vendor flaw remediation activities); and
- developing an assessment plan

## Assessment Results

For each security requirement question that the company answers **Yes**, a statement should be included in the Security Assessment Report and System Security Plan which explains how the information system implements the requirement.

For each security requirement question that the company answers **No**, a statement should be included in the Security Assessment Report which explains why the security requirement is not met. A statement should also be included in the Plan of Action which fully describes how the unimplemented security requirements will be met, how any planned improvements will be implemented, and when the improvements will occur.

For each security requirement questions that the company answers **Partially**, a statement should be included in the Security Assessment Report which explains why the security requirement is partially met. A statement should also be included in the Plan of Action which fully describes how the partially met security requirements will be fully met, how any planned improvements will be implemented and when the improvements will occur.

For each security requirement question that the company answers **Does Not Apply**, a statement should be included in the Security Assessment Report which explains why the security requirement does not apply to your operational environment.

For each security requirement question that the company answers **Alternative Approach**, a statement should be included in the Security Assessment Report and in the System Security Plan which fully describes the alternative approach and how it is equally effective. A statement should also be included that explains how the information system implements the requirement.

## Self-Assessment Handbook

### Access Control: SP 800-171 Security Family 3.1

Access is the ability to make use of any system resource. Access control is the process of granting or denying requests to:

- use information,
- use information processing services, and
- enter company facilities.

System-based access controls are called logical access controls. Logical access controls prescribe not only who or what (in the case of a process) is permitted to have access to a system resource, but also the type of access that is permitted. These controls may be built into the operating system, incorporated into applications programs or major utilities (e.g., database management systems, communications systems), or implemented through add-on security packages. Logical access controls may be implemented internally to the system being protected or in external devices. Examples of access control security requirements include account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination.

Companies should limit:

- system access to authorized users,
- processes acting on behalf of authorized users,
- devices, including other systems, and
- the types of transactions and functions that authorized users are permitted to exercise.

The requirements for using – and prohibitions against the use of – various system resources can vary from one system to another. For example, some information must be accessible to all users, some may be needed by several groups or departments, and some may only be accessed by a few individuals within the company. While users must have access to specific information needed to perform their jobs, denial of access to non-job-related information may be required. It may also be important to control the kind of access that is permitted (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken.

Controlling physical access to company facilities is also important. It provides for the protection of employees, plant equipment, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to the company. This includes burglary, theft, vandalism, and terrorism.

The following security requirements fall under the Access Control family.

### 3.1.1 *Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).*

Does the company use passwords?

Yes No Partially Does Not Apply Alternative Approach

Does the company have an authentication mechanism?

Yes No Partially Does Not Apply Alternative Approach

Does the company require users to logon to gain access?

Yes No Partially Does Not Apply Alternative Approach

Are account requests authorized before system access is granted?

Yes No Partially Does Not Apply Alternative Approach

Does the company maintain a list of authorized users, defining their identity and role and sync with system, application, and data layers?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional information:**

User access security refers to the set of procedures by which authorized users access the system and unauthorized users are prevented accessing the system.

#### **Where to Look:**

- access control policy
- account management procedures
- access enforcement procedures
- security plan
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of active system accounts along with the name of the individual associated with each account
- list of conditions for group and role membership
- notifications or records of recently transferred, separated, or terminated employees

- list of recently disabled information system accounts along with the name of the individual associated with each account
- list of approved authorizations (user privileges)
- access authorization records
- account management compliance reviews
- information system monitoring records
- information system audit records
- remote access implementation and usage (including restrictions) procedures
- remote access authorizations

#### **Who to Talk to:**

- employees with account management responsibilities
- system/network administrators
- employees with responsibilities for managing remote access connections
- employees with information security responsibilities
- employees with access enforcement responsibilities
- system developers

#### **Perform Test On:**

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability

### 3.1.2 *Limit system access to the types of transactions and functions that authorized users are permitted to execute.*

Do you use access control lists to limit access to applications and data based on role and/or identity?

Yes No Partially Does Not Apply Alternative Approach

Does the system allow for the separation of access control rights and enforcement of those rights?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional information:**

Even authorized users are restricted to those parts of the system that they are explicitly permitted to use. This is based on their “need-to-know” and their role within the company.

#### **Where to Look:**

- access control policy
- account management procedures
- access enforcement procedures
- security plan
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of active system accounts along with the name of the individual associated with each account
- list of conditions for group and role membership notifications or records of recently transferred, separated, or terminated employees
- list of recently disabled information system
- accounts along with the name of the individual associated with each account
- list of approved authorizations (user privileges)
- access authorization records
- account management compliance reviews
- information system monitoring records
- information system audit records

- procedures addressing remote access implementation and usage (including restrictions)
- remote access authorizations

#### **Who to Talk to:**

- personnel with account management responsibilities
- system/network administrators
- personnel with responsibilities for managing remote access connections
- personnel with information security responsibilities
- personnel with access enforcement responsibilities
- system developers

#### **Perform Test On:**

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability for the information system

### 3.1.3 Control the flow of CUI in accordance with approved authorizations.

Do you have architectural solutions to control the flow of system data?

Yes No Partially Does Not Apply Alternative Approach

Do you document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The solutions may include firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who is allowed to access the information) without explicit regard to subsequent accesses to that information.

Examples of flow control restrictions include:

- keeping export-controlled information from being transmitted in the clear to the internet,
- blocking outside traffic that claims to be from within the organization,
- restricting web requests to the internet that are not from the internal web proxy server, and
- limiting information transfers between organizations based on data structures and content.

Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. The company may consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example:

- prohibiting information transfers between interconnected systems (i.e., allowing access only),
- employing hardware mechanisms to enforce one-way information flows, and

- implementing trustworthy regrading mechanisms to reassign security attributes and security label.

Companies commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Companies may also consider the trustworthiness of filtering/ inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

#### Where to Look:

- access control policy
- information flow control policies
- procedures addressing information flow enforcement
- information system design documentation
- information system configuration settings and associated documentation
- information system baseline configuration
- list of information flow authorizations  
information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

#### Perform Test On:

- automated mechanisms implementing information flow enforcement policy



### 3.1.4 *Separate the duties of individuals to reduce the risk of malevolent activity without collusion.*

If a user accesses data as well as maintains the system in some way, do you create separate accounts with appropriate access levels to separate functions?

Yes No Partially Does Not Apply Alternative Approach

Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information:**

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separations of duties includes:

- Dividing mission functions and information support functions among different individuals and/or roles,
- Conducting information system support functions with different individuals (systems management, programming, configuration management, quality assurance and testing, and network security), and
- Ensuring security personnel administering access control functions do not also administer audit functions.

#### **Where to Look:**

- access control policy
- procedures addressing divisions of responsibility and separation of duties
- information system configuration settings and associated documentation
- list of divisions of responsibility and separation of duties
- information system access authorizations
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for defining appropriate divisions of responsibility and

separation of duties

- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- automated mechanisms implementing separation of duties policy

### 3.1.5 *Employ the principle of least privilege, including for specific security functions and privileged accounts.*

Do you only grant enough privileges to users to allow them to do their job?

Yes No Partially Does Not Apply Alternative Approach

Does the company restrict access to privileged functions and security information to authorized employees?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional information:**

The principle of least privilege requires that every process, user, or program can only access the information and resources that are needed for its valid purpose. The principle of least privilege means giving a process, program, or user account only those privileges that are essential for it to perform its intended function.

When applied to users, the term least-privileged user account (LUA) is also used. Meaning all user accounts should always run with as few privileges as possible, and launch applications with as few privileges as possible.

#### **Where to Look:**

- access control policy
- procedures addressing least privilege
- list of assigned access authorizations (user privileges)
- list of system generated privileged accounts
- list of system administration personnel
- information system configuration settings and associated documentation
- list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for defining least privileges necessary to accomplish specified tasks

- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- automated mechanisms implementing least privilege functions

### 3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

Do users with multiple accounts (privileged and non-privileged) typically logon with the least privileged account when not performing privileged functions?

Yes No Partially Does Not Apply Alternative Approach

Can this be described or demonstrated?

Yes No Partially Does Not Apply Alternative Approach

Are users with privileged access required to use non-privileged accounts when accessing other system functions?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where companies implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Note that the privileged account should not be used to do non-privileged functions.

NIST SP 800-171 defines a “privileged user” as “a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.” For example, if users’ computer accounts are “administrator accounts” or have “limited administrative rights” only on their computers, are they considered a “privileged account” requiring audit for privileged functions? Since, in this case, the “ordinary users” are authorized to perform the function, they are not considered privileged users.

#### Where to Look:

- access control policy
- procedures addressing least privilege
- list of system generated security functions or security-relevant information assigned to information system accounts or roles
- information system configuration settings and associated documentation
- information system audit records other relevant documents or records

#### Who to Talk to:

- employees with responsibilities for defining least privileges necessary to accomplish specified tasks
- employees with information security responsibilities
- system/network administrators

#### Perform Test On:

- automated mechanisms implementing least privilege functions

### 3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

Do you enable auditing of all privileged functions?

Yes No Partially Does Not Apply Alternative Approach

Do you prevent the execution of privileged functions by non-privileged users?

Yes No Partially Does Not Apply Alternative Approach

Do you control access using access control lists based on the identity or role of the user?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

NIST SP 800-171 defines a “privileged user” as “a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.” For example, if users’ computer accounts are “administrator accounts” or have “limited administrative rights” only on their computers, they are not considered a “privileged account” requiring audit for privileged functions. Since, in this case, the “ordinary users” are authorized to perform the function, they are not considered privileged users.

#### Where to Look:

- access control policy
- procedures addressing least privilege
- information system design documentation

- information system configuration settings and associated documentation
- list of privileged functions to be audited
- list of privileged functions and associated user account assignments
- list of audited events
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with responsibilities for reviewing least privileges necessary to accomplish specified tasks
- employees with responsibilities for defining least privileges necessary to accomplish specified tasks
- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- automated mechanisms auditing the execution of least privilege functions
- automated mechanisms implementing least privilege functions for non-privileged users

### 3.1.8 Limit unsuccessful logon attempts.

Is the system configured to limit the number of invalid logon attempts?

Yes No Partially Does Not Apply Alternative Approach

Is the system configured to lock the logon mechanism for a predetermined time after a predetermined number of invalid logon attempts?

Yes No Partially Does Not Apply Alternative Approach

Is the system configured to lock users out after a predetermined number of invalid logon attempts?

Yes No Partially Does Not Apply Alternative Approach

Does the system enforce a limit of a defined number of consecutive invalid access attempts during a defined time?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement seeks to limit the number of logon attempts. Multiple unsuccessful logon attempts may indicate malicious attacks on the information system.

#### Where to Look:

- access control policy
- procedures addressing unsuccessful logon attempts
- security plan
- information system design documentation
- information system configuration settings and associated documentation information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with information security responsibilities
- system developers
- system/network administrators

#### Perform Test On:

- automated mechanisms implementing access control policy for unsuccessful logon attempts

### 3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

Does the logon screen display notices upon initial logon?

Yes No Partially Does Not Apply Alternative Approach

Does the system display the system use information before granting access?

Yes No Partially Does Not Apply Alternative Approach

Does the system ensure that any references to monitoring, recording, or auditing are consistent with privacy accommodations?

Yes No Partially Does Not Apply Alternative Approach

Does the system include a description of the authorized uses of the system?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Companies may consider system use notification messages/ banners displayed in multiple languages based on specific company needs and the demographics of information system users.

This requirement references the National Archives and Records Administration's (NARA) Federal Rule 32 CFR 2002 implementing its CUI program. It applies if a specific type of CUI (i.e., information that requires safeguarding or dissemination controls pursuant to law, regulation or Government-wide policy) requires such notices (e.g., before accessing or entering the data. This is not a common situation.

#### Where to Look:

- information system design documentation
- information system configuration settings and associated documentation
- information system notification messages
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- system developers

- employees with information security responsibilities

#### Perform Test On:

- automated mechanisms implementing access control policy for previous logon notification

### 3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.

Is the system configured to lock sessions after a predetermined period of inactivity?

Yes No Partially Does Not Apply Alternative Approach

Is a pattern hiding display used when sessions are locked?

Yes No Partially Does Not Apply Alternative Approach

Can users lock sessions for temporary absence?

Yes No Partially Does Not Apply Alternative Approach

Does the system session lock mechanism place a publicly viewable pattern onto the screen? Hiding what was previously visible on the screen?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Pattern-hiding display images can include static or dynamic images, for example patterns used with screen savers, photographic images, clock, battery life indicator, or a blank screen with the additional caveat that none of the images convey sensitive information.

#### Where to Look:

- access control policy
- procedures addressing session lock
- display screen with session lock activated
- procedures addressing identification and authentication
- information system design documentation
- information system configuration settings and associated documentation
- security plan
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

#### Perform Test On:

- automated mechanisms implementing access control policy for session lock
- information system session lock mechanisms

### 3.1.11 *Terminate (automatically) a user session after a defined condition.*

Is the system configured to end a user session after a predetermined period based on duration and/or inactivity of session?

Yes No Partially Does Not Apply Alternative Approach

Are user sessions terminated automatically based upon company defined conditions? For example, 10 minute timeouts?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This requirement addresses the termination of user-initiated logical sessions in contrast to other requirements that address the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses a company information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

#### **Where to Look:**

- access control policy
- procedures addressing session termination
- information system design documentation
- information system configuration settings and associated documentation
- list of conditions or trigger events requiring session disconnect
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security

responsibilities

- system developers

#### **Perform Test On:**

- automated mechanisms implementing user session termination



### 3.1.12 Monitor and control remote access sessions.

Does the company allow remote access to the control network?

Yes No Partially Does Not Apply Alternative Approach

Do you run network and system monitoring applications to monitor remote system access and log accordingly?

Yes No Partially Does Not Apply Alternative Approach

Do you control remote access by running only necessary applications?

Yes No Partially Does Not Apply Alternative Approach

Do you use firewalling?

Yes No Partially Does Not Apply Alternative Approach

Do you use end-to-end encryption with appropriate access?

Yes No Partially Does Not Apply Alternative Approach

Are all the methods of remote access to the system authorized, monitored, and managed?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Remote access is access to a company's IT system by a user communicating through an external network such as the internet.

Remote access client devices generally have weaker protection than standard client devices. These may include:

- Many devices are not managed by the company and do not use enterprise firewalls or antivirus protection.
- A lack of physical security controls when using remote access.
- Remote access client devices may be used in hostile environments but not properly configured for them.
- Remote access communications are carried over untrusted networks.

It is useful to note that one can "monitor and control remote access" by not providing the capability and employing procedural methods to ensure it has not been enabled.

#### Where to Look:

- access control policy
- procedures addressing remote access to the information system
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- information system monitoring records
- other relevant documents or record

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

#### Perform Test On:

- automated mechanisms monitoring and controlling remote access methods

### 3.1.13 *Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.*

Do applications used to remotely access the system use approved encryption methods?

Yes No Partially Does Not Apply Alternative Approach

Is cryptography used to protect the confidentiality and integrity of remote access sessions?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use Federal Information Processing Standard (FIPS) validated cryptography, which means the cryptographic module has been tested and validated to meet FIPS 140 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at <http://csrc.nist.gov/groups/STM/cmvp/>

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the company's information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., Personally Identifiable Information - PII) within the information system would require use of FIPS-validated cryptography.

#### **Where to Look:**

- access control policy

- procedures addressing remote access to the information system
- information system design documentation
- information system configuration settings and associated documentation
- cryptographic mechanisms and associated configuration documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- system developers

#### **Perform Test On:**

- cryptographic mechanisms protecting confidentiality and integrity of remote access sessions

### 3.1.14 *Route remote access via managed access control points.*

Do you allow remote access?

Yes No Partially Does Not Apply Alternative Approach

Is remote access only allowed by authorized methods?

Yes No Partially Does Not Apply Alternative Approach

Is remote access only maintained by your IT department?

Yes No Partially Does Not Apply Alternative Approach

Does the system route all remote access through a limited number of managed access control points?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Companies should identify and fully define the number of managed network access control points used for remote accesses are routed. All remote access to the system should be routed through these company's managed network access control points.

#### **Where to Look:**

- access control policy
- procedures addressing remote access to the information system
- information system design documentation
- list of all managed network access control points
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms routing all remote accesses through managed network access control point

### **3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.**

Is remote access for privileged actions (such as software installation) only permitted for necessary operational functions?

Yes No Partially Does Not Apply Alternative Approach

Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This security requirement is intended to limited the use of remote access to perform privileged actions on the system. Privileged commands are human initiated and involve the control, monitoring or administration of the system and security functions.

#### **Where to Look:**

- access control policy
- procedures addressing remote access to the information
- information system configuration settings and associated documentation
- security plan
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms implementing remote access management

### 3.1.16 *Authorize wireless access prior to allowing such connections.*

Does the company have wireless devices?

Yes No Partially Does Not Apply Alternative Approach

Is the use of wireless technologies approved by company management?

Yes No Partially Does Not Apply Alternative Approach

Is there guidance on the use of wireless technologies?

Yes No Partially Does Not Apply Alternative Approach

Is access to the wireless network restricted to the established guidelines, monitored, and controlled?

Yes No Partially Does Not Apply Alternative Approach

Is wireless access to the system authorized, monitored and managed?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

The use of wireless devices on company systems should be based on management approved guidelines. Access to the wireless network should be monitored and controlled by the company.

#### **Where to Look:**

- access control policy
- procedures addressing wireless access implementation and usage (including restrictions)
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- wireless access authorizations
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for managing wireless access connections
- employees with information security responsibilities

#### **Perform Test On:**

- wireless access management capability for the information system

### 3.1.17 *Protect wireless access using authentication and encryption.*

Is wireless access restricted to authorized users?

Yes No Partially Does Not Apply Alternative Approach

Is wireless access encrypted according to industry best practices?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module has been tested and validated to meet FIPS 140 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/ or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

<http://csrc.nist.gov/groups/STM/cmvp/>

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the company's information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision.

Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS-validated cryptography.

#### **Where to Look:**

- access control policy
- procedures addressing wireless implementation and usage (including restrictions)
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- system developers

#### **Perform Test On:**

- automated mechanisms implementing wireless access protections to the information system

### 3.1.18 Control connection of mobile devices.

Has company management established guidelines for the use of mobile devices?

Yes No Partially Does Not Apply Alternative Approach

Does company management restrict the operation of those devices to the guidelines?

Yes No Partially Does Not Apply Alternative Approach

Is usage monitored and controlled?

Yes No Partially Does Not Apply Alternative Approach

Is mobile device connection to the system authorized?

Yes No Partially Does Not Apply Alternative Approach

Are requirements for mobile device connection to the system enforced?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Mobile devices allow employees to access information resources wherever they are, whenever they need. The small form factor, constant internet access, and powerful mobile applications greatly improve workforce productivity but can pose cybersecurity risks. While many only think of smartphones as mobile devices, companies must consider the security of all mobile network devices including tablets and laptops used as workstations.

NISTIR 8144 “Assessing Threats to Mobile Devices & Infrastructure” describes, identifies, and structures the threats posed to mobile information systems, and can be accessed at

<https://nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf>

NIST SP 800-124 Rev. 1 “Guidelines for Managing Security of Mobile Devices in the Enterprise” helps organizations centrally manage and secure mobile devices against a variety of threats. It provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use.

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>

#### Where to Look:

- access control policy
- procedures addressing access control for mobile device usage (including restrictions)
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- authorizations for mobile device connections to company information systems
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees using mobile devices to access
- system/network administrators
- employees with information security responsibilities

#### Perform Test On:

- access control capability authorizing mobile device connections to company information systems

### 3.1.19 Encrypt CUI on mobile devices.

Are mobile devices encrypted?

Yes No Partially Does Not Apply Alternative Approach

Does the company encrypt CUI on mobile devices?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module should have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient - the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

<http://csrc.nist.gov/groups/STM/cmvp/>

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the company's information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption

is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS-validated cryptography.

#### Where to Look:

- access control policy
- procedures addressing access control for mobile devices
- information system design documentation

- information system configuration settings and associated documentation
- encryption mechanisms and associated configuration documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with access control responsibilities for mobile devices system/network administrators
- employees with information security responsibilities

#### Perform Test On:

- encryption mechanisms protecting confidentiality and integrity of information on mobile devices



### 3.1.20 *Verify and control/limit connections to and use of external information systems.*

Are only authorized individuals permitted external access?

Yes No Partially Does Not Apply Alternative Approach

Are guidelines and restrictions placed on the use of personally owned or external system access?

Yes No Partially Does Not Apply Alternative Approach

Do those systems meet the security standards set by the company?

Yes No Partially Does Not Apply Alternative Approach

Are the number of access points to the system limited to allow for better monitoring of inbound and outbound network traffic?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the company. Companies typically have no direct supervision and authority over the application of security requirements or the assessment of their effectiveness in external information systems. External information systems include, for example: 1) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); 2) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); 3) information systems owned or controlled by nonfederal governmental organizations; and 4) federal information systems that are not owned by, operated by, or under the direct supervision and authority of companies.

#### **Where to Look:**

- access control policy procedures addressing the use of external information systems
- external information systems terms and conditions
- list of types of applications accessible from external information systems
- maximum security categorization for information processed, stored, or transmitted on external information systems
- information system configuration settings and associated documentation
- information system connection or processing agreements
- account management documents
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for defining terms and conditions for use of external information systems to access company systems
- system/network administrators
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms implementing terms and conditions on use of external information systems
- automated mechanisms implementing limits on use of external information systems

### 3.1.21 *Limit use of organization portable storage devices on external information systems.*

Are guidelines and restrictions placed on the use of portable storage devices, e.g., thumb drives?

Yes No Partially Does Not Apply Alternative Approach

Are restrictions imposed on authorized individuals regarding the use of company-controlled removable media on external systems?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

A ‘portable storage device’ is an information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Limits on the use of company-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

This requirement is generally implemented by policy, though some devices can be configured to work only when connected to a system to which they can authenticate (this is, however, not a requirement).

#### **Where to Look:**

- access control policy
- procedures addressing the use of external information systems
- security plan
- information system configuration settings and associated documentation
- information system connection or processing agreements
- account management documents
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for restricting or prohibiting use of company controlled storage devices on external information systems
- system/network administrators
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms restricting use of portable storage devices

### 3.1.22 Control CUI posted or processed on publicly accessible information systems.

Do only authorized employees post information on publicly accessible information systems?

Yes No Partially Does Not Apply Alternative Approach

Are authorized employees trained to ensure that CUI and non-public information is not posted?

Yes No Partially Does Not Apply Alternative Approach

Is public information reviewed annually to ensure that CUI and non-public information is not posted?

Yes No Partially Does Not Apply Alternative Approach

Is the proposed content of publicly accessible information reviewed prior to posting?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Improper use of the company's proprietary information can damage the company. Improper use of CUI could cause damage to the government and/or its employees.

This requirement addresses systems that are controlled by the company and accessible to the public, typically without identification or authentication. The posting of information on non-organization information systems is covered by company policy.

DOD uses a variety of markings to identify CUI, identified in DOD Manual 5200.01 Vol 4, which will be updated as the NARA CUI rule (32 CFR 2002) is implemented. The most common form of DOD CUI held by contractors is Controlled Technical Information, which is marked with Distribution Statements B-F. Other DOD information may be marked as 'For Official Use Only' – which may or may not be CUI, and the contracting officer should be consulted if this marking is encountered to determine if it is DOD CUI.

#### Where to Look:

- access control policy
- procedures addressing publicly accessible content
- list of users authorized to post publicly accessible content on company information systems
- training materials and/or records
- records of publicly accessible information reviews
- records of response to nonpublic information on public websites
- system audit logs
- security awareness training records
- other relevant documents or records

#### Who to Talk to:

- employees with responsibilities for managing publicly accessible information posted on company information systems
- employees with information security responsibilities

#### Perform Test On:

- automated mechanisms implementing management of publicly accessible content

## **Awareness and Training: SP 800-171 Security Family 3.2**

Users of a system can be viewed as the weakest link in securing systems. Often users are not aware of how their actions may impact the security of a system. Making system users aware of their security responsibilities and teaching them correct practices helps change their behavior. It also supports individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures or how to use them, users cannot be truly accountable for their actions.

The purpose of information security awareness, training, and education is to enhance security by:

- raising awareness of the need to protect system resources,
- developing skills and knowledge so system users can perform their jobs more securely, and
- building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems.

The company is responsible for making sure that managers and users are aware of the security risks associated with their activities and that employees are trained to carry out their information security-related duties and responsibilities. Examples of awareness and training security requirements include: security awareness training, role based security training, and security training records.

The following security requirements fall under the Awareness and Training family.

### 3.2.1 *Ensure that managers, systems administrators, and users of organization information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organization information systems.*

Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities?

Yes No Partially Does Not Apply Alternative Approach

Does the training provide a basic understanding of the need for information security, applicable policies, standards, and procedures related to the security of the information system, as well as user actions to maintain security and respond to suspected security incidents?

Yes No Partially Does Not Apply Alternative Approach

Does the training also address awareness of the need for operations security?

Yes No Partially Does Not Apply Alternative Approach

Is basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Companies determine the appropriate content of security awareness training and security awareness techniques based on the specific company requirements and the information systems to which employees have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior company officials, displaying logon screen messages, and conducting information security awareness events.

#### **Where to Look:**

- security awareness and training policy
- procedures addressing security awareness

training implementation

- appropriate codes of federal regulations
- security awareness training curriculum
- security awareness training materials
- security plan
- training records
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for security awareness training
- employees with information security responsibilities
- employees comprising the general information system user community
- employees with responsibilities for role-based security training

#### **Perform Test On:**

- automated mechanisms managing security awareness training
- automated mechanisms managing role-based security training

### 3.2.2 *Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.*

Do employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities?

Yes No Partially Does Not Apply Alternative Approach

Does the training cover physical, personnel, and technical safeguards and countermeasures?

Yes No Partially Does Not Apply Alternative Approach

Does the training address required security requirements related to environmental and physical security risks?

Yes No Partially Does Not Apply Alternative Approach

Does the training include indications of potentially suspicious email or web communications?

Yes No Partially Does Not Apply Alternative Approach

Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on a periodic basis?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Companies determine the appropriate content of security training based on the assigned roles and responsibilities of individuals, and the specific security requirements of companies

and the information systems to which personnel have authorized access. In addition, companies provide enterprise architects, information system developers, software developers, acquisition/ procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security requirement assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the company security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of company information security programs. Role-based security training also applies to contractors providing services to federal agencies.

#### **Where to Look:**

- security awareness and training policy
- procedures addressing security awareness training implementation
- appropriate codes of federal regulations
- security awareness training curriculum
- security awareness training materials
- security plan training records
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for security awareness training
- employees with information security responsibilities
- employees with responsibilities for role-based security training
- employees with assigned information system security roles and responsibilities
- employees comprising the general information system user community

#### **Perform Test On:**

- automated mechanisms managing security awareness training
- automated mechanisms managing role-based security training

### 3.2.3 *Provide security awareness training on recognizing and reporting potential indicators of insider threat.*

Do users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threat, e.g., long-term job dissatisfaction, attempts to gain unauthorized access to information, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies?

Yes No Partially Does Not Apply Alternative Approach

Does security training include how to communicate employee and management concerns regarding potential indicators of insider threat?

Yes No Partially Does Not Apply Alternative Approach

Are practical exercises included in security awareness training that simulate actual cyber-attacks?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Potential indicators and possible precursors of insider threat can include behaviors such as long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies, procedures, directives, rules, or practice. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate company channels in accordance with established company policies and procedures.

#### **Where to Look:**

- security awareness and training policy
- procedures addressing security awareness training implementations
- security awareness training curriculum
- security awareness training materials
- security plan
- other relevant documents or records

#### **Who to Talk to:**

- employees who participate in security awareness training
- employees with responsibilities for basic security awareness training
- employees with information security responsibilities

### **Audit and Accountability: SP 800-171 Security Family 3.3**

An audit is an independent review and examination of records and activities to assess the adequacy of system requirements and ensure compliance with established policies and operational procedures.

An audit trail is a record of individuals who have accessed a system as well as what operations the user has performed during a given period. Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance issues, and flaws in applications. Audit trails may be used as a support for regular system operations, a kind of insurance policy, or both. As insurance, audit trails are maintained but not used unless needed (e.g., after a system outage). As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems. Examples of audit and accountability requirements include: audit events, time stamps, nonrepudiation, protection of audit information, audit record retention, and session audit.

Companies should create, protect, and retain 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 users can be uniquely traced to those users so they can be held accountable.

The following security requirements fall under the Audit and Accountability family.



**3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.**

Does the system provide alert functions?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform audit analysis and review?

Yes No Partially Does Not Apply Alternative Approach

Does the company create, protect, and retain information system audit records for between 30 days and 1 year (depending on data source and applicable regulations) to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity?

Yes No Partially Does Not Apply Alternative Approach

Are mechanisms used to integrate audit review, analysis, and reporting to processes for investigation and response to suspicious activity?

Yes No Partially Does Not Apply Alternative Approach

**Additional Information**

It is important for companies to create audit records, protect the integrity of audit records and retain audit records. Good audit records will allow the company to monitor system activities, perform analysis on system activities, provide evidence for use during an investigation and reporting.

**Where to Look:**

- audit and accountability policy
- procedures addressing content of audit records
- information system design documentation
- procedures addressing audit record generation
- security plan
- list of auditable events
- information system configuration settings and associated documentation

- list of organization-defined auditable events
- information system audit records
- procedures addressing audit review, analysis, and reporting
- reports of audit findings
- records of actions taken in response to reviews/analyses of audit records
- information system incident reports
- other relevant documents or records

**Who to Talk to:**

- employees with audit and accountability responsibilities
- employees with audit review, analysis, and reporting responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

**Perform Test On:**

- automated mechanisms implementing information system auditing of auditable events
- information system audit capability

### 3.3.2 *Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.*

Does the company correlate network activity to individual user information?

Yes No Partially Does Not Apply Alternative Approach

Can the company uniquely trace and hold accountable users responsible for unauthorized actions?

Yes No Partially Does Not Apply Alternative Approach

Does the system protect against an individual denying having performed an action (non-repudiation)?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by:

- authors of not having authored documents,
- senders of not having transmitted messages,
- receivers of not having received messages, or
- signatories of not having signed documents.

Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Companies obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

#### **Where to Look:**

- audit and accountability policy
- procedures addressing content of audit records
- information system design documentation
- procedures addressing audit record generation

- security plan
- list of auditable events
- information system configuration settings and associated documentation
- list of organization-defined auditable events
- information system audit records
- procedures addressing audit review, analysis, and reporting
- reports of audit findings
- records of actions taken in response to reviews/analyses of audit records
- information system incident reports
- other relevant documents or records

#### **Who to Talk to:**

- employees with audit and accountability responsibilities
- employees with audit review, analysis, and reporting responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### **Perform Test On:**

- automated mechanisms implementing information system auditing of auditable events
- information system audit capability

### 3.3.3 *Review and update audited events.*

Does the company review and update audited events annually or in the event of substantial system changes or as needed?

Yes No Partially Does Not Apply Alternative Approach

Do reviews ensure that the information system can audit events, coordinate with other company entities requiring audit-related information, and provide a rationale for why auditable events are deemed adequate to support security investigations?

Yes No Partially Does Not Apply Alternative Approach

Is the list of defined auditable events reviewed by company management and updated on a regular basis?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Over time, the events that companies believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

#### **Where to Look:**

- audit and accountability policy
- procedures addressing auditable events
- security plan
- list of organization-defined auditable events
- auditable events review and update records
- information system audit records
- information system incident reports
- other relevant documents or records

#### **Who to Talk to:**

- employees with audit and accountability responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms supporting review and update of auditable events

### 3.3.4 Alert in the event of an audit process failure.

Will the system alert employees with security responsibilities in the event of an audit processing failure?

Yes No Partially Does Not Apply Alternative Approach

Does the system maintain audit records on host servers until log delivery to central repositories can be re-established?

Yes No Partially Does Not Apply Alternative Approach

Is there real-time alert when any defined event occurs?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

An accurate and current audit trail is essential for maintaining a record of system activity. If the system fails, employees with security responsibilities must be notified and must take prompt action to correct the problem. Minimally, the system must log this event and the employees with security responsibilities (e.g., system administrator) will receive this notification during the daily system log review. If feasible, active alerting (such as e-mail or paging) should be employed consistent with the company's established operations management systems and procedures.

#### Where to Look:

- audit and accountability policy
- procedures addressing response to audit processing failures
- information system design documentation
- security plan
- information system configuration settings and associated documentation
- list of personnel to be notified in case of an audit processing failure
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with audit and accountability responsibilities
- employees with information security responsibilities
- system/network administrator's system developers

#### Perform Test On:

- automated mechanisms implementing information system response to audit processing failures

### 3.3.5 *Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.*

Does the company use mechanisms across different repositories to integrate audit review, analysis, correlation, and reporting processes?

Yes No Partially Does Not Apply Alternative Approach

Do the mechanisms support processes for investigation and response to suspicious activities, as well as gain company-wide situational awareness?

Yes No Partially Does Not Apply Alternative Approach

Are mechanisms used to integrate audit review, analysis and reporting to processes for investigation and response to suspicious activity?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Often small companies do a good job of collecting audit information across different platforms but fail to correlate the review, analysis and reporting processes. Providing connections and relationships in the audit information can greatly help in the investigation of and response to suspicious activity on the system.

#### **Where to Look:**

- audit and accountability policy
- procedures addressing audit review, analysis, and reporting
- procedures addressing investigation and response to suspicious activities
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- information system audit records across different repositories
- other relevant documents or records

#### **Who to Talk to:**

- employees with audit review, analysis, and reporting responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms integrating audit review, analysis, and reporting processes
- automated mechanisms supporting analysis and correlation of audit records

### 3.3.6 *Provide audit reduction and report generation to support on-demand analysis and reporting.*

Does the system provide an audit reduction and report generation capability?

Yes No Partially Does Not Apply Alternative Approach

Does it support on-demand audit review, analysis, and reporting requirements and after-the-fact security investigations?

Yes No Partially Does Not Apply Alternative Approach

Does the information system alter the original content or time-ordering of audit records?

Yes No Partially Does Not Apply Alternative Approach

Is there the capability to process audit records for events of interest based on selectable event criteria, such as user identity, event type, location, times, dates, system resources, IP, or information object accessed?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to reviewers. Audit reduction and report generation capabilities do not always come from the same information system or from the same company entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.

The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the details of the timestamp in the record are insufficient.

#### **Where to Look:**

- audit and accountability policy
- procedures addressing audit reduction and report generation
- information system design documentation
- information system configuration settings and associated documentation
- audit reduction, review, analysis, and reporting tools
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with audit reduction and report generation responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- audit reduction and report generation capability

**3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.**

internal information system clock synchronization

Does the system use internal system clocks to generate time stamps for audit records?

Yes No Partially Does Not Apply Alternative Approach

Can the records time stamps be mapped to UTC (Coordinated Universal Time), compare system clocks with authoritative NTP (Network Time Protocol) servers, and synchronizes system clocks when the time difference is greater than 1 second?

Yes No Partially Does Not Apply Alternative Approach

Does the system synchronize internal system clocks on a defined frequency?

Yes No Partially Does Not Apply Alternative Approach

**Additional Information**

This provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

**Where to Look:**

- audit and accountability policy
- procedures addressing time stamp generation information
- system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

**Who to Talk to:**

- employees with information security responsibilities
- system/network administrators
- system developers

**Perform Test On:**

- automated mechanisms implementing time stamp generation
- automated mechanisms implementing

### 3.3.8 *Protect audit information and audit tools from unauthorized access, modification, and deletion.*

Does the system protect audit information and audit tools from unauthorized access, modification, and deletion?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This security requirement seeks to prevent a malicious user from erasing all evidence of their activities in the audit information. Only authorized users should have access to audit information and audit tools.

#### **Where to Look:**

- audit and accountability policy
- access control policy and procedures
- procedures addressing protection of audit information

- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- audit tools
- other relevant documents or records

#### **Who to Talk to:**

- employees with audit and accountability responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### **Perform Test On:**

- automated mechanisms implementing audit information protection



### 3.3.9 *Limit management of audit functionality to a subset of privileged users.*

Is access to management of audit functionality authorized only to a limited subset of privileged users?

Yes No Partially Does Not Apply Alternative Approach

Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This requires that privileged access be further defined between audit-related privileges and other privileges, limiting the users with audit-related privileges.

#### **Where to Look:**

- audit and accountability policy
- access control policy and procedures
- procedures addressing protection of audit information
- information system design documentation
- information system configuration settings and associated documentation,
- system-generated list of privileged users with access to management of audit functionality
- access authorizations
- access control list
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with audit and accountability responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- automated mechanisms managing access to audit functionality

### **Configuration Management: SP 800-171 Security Family 3.4**

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC). Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a change control board. It allows the entire system to be reviewed to help ensure that a change made on one system does not have adverse effects on another system.

Common secure configurations (also known as security configuration checklists) provide recognized, standardized, and established benchmarks that specify secure configuration settings for information technology platforms and products. Once implemented, checklists can be used to verify that changes to the system have been reviewed from a security point-of-view. A common audit examines the system's configuration to see if major changes (such as connecting to the internet) have occurred that have not yet been analyzed. The NIST checklist repository, maintained as part of the National Vulnerability Database (NVD), provides multiple checklists which can be used to check compliance with the secure configuration specified in the system security plan. The checklists can be accessed at <http://web.nvd.nist.gov/view/ncp/repository>.

Examples of configuration management requirements include baseline configuration, configuration change control, security impact analysis, least functionality, and software usage restrictions.

Companies establish and maintain baseline configurations and inventories of company systems, including hardware, software, firmware, and documentation throughout the respective SDLC and establish and enforce security configuration settings for information technology products employed in company systems.

The following security requirements fall under the Configuration Management family.

### 3.4.1 Establish and maintain baseline configurations and inventories of organization information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Are baseline configurations developed, documented, and maintained for each information system type?

Yes No Partially Does Not Apply Alternative Approach

Do baseline configurations include software versions and patch level, configuration parameters, network information including topologies, and communications with connected systems?

Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations updated as needed to accommodate security risks or software changes?

Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations developed and approved in conjunction with the Chief Information Security Officer (CISO) or equivalent and the information system owner?

Yes No Partially Does Not Apply Alternative Approach

Are deviations from baseline configurations documented?

Yes No Partially Does Not Apply Alternative Approach

Is the system managed using a system development life-cycle methodology that includes security considerations?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of company information systems. To apply the required security requirements within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. Security engineering cannot be properly applied if individuals who design, code, and test information systems and system components (including information technology products) do not understand security. It is important that developers include individuals on the development team who possess security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and

training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the company's business processes. This process also enables the integration of the information security architecture into the enterprise architecture, consistent with company risk management and information security strategies.

#### Where to Look:

- configuration management policy
- procedures addressing the baseline configuration of the information system
- procedures addressing configuration settings for the information system
- configuration management plan
- security plan
- enterprise architecture documentation
- security configuration checklists
- evidence supporting approved deviations from established configuration settings
- change control records
- information system audit records
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- change control records
- other relevant documents or records

#### Who to Talk to:

- employees with configuration management responsibilities
- employees with security configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

**Perform Test On:**

- processes for managing baseline configurations
- automated mechanisms supporting configuration control of the baseline configuration
- processes for managing configuration settings
- automated mechanisms that implement, monitor, and/or control information system configuration settings
- automated mechanisms that identify and/ or document deviations from established configuration settings

### 3.4.2 Establish and enforce security configuration settings for information technology products employed in organization information systems.

Are security settings included as part of baseline configurations?

Yes No Partially Does Not Apply Alternative Approach

Do security settings reflect the most restrictive settings appropriate?

Yes No Partially Does Not Apply Alternative Approach

Are changes or deviations to security settings documented?

Yes No Partially Does Not Apply Alternative Approach

#### Where to Look:

- configuration management policy
- procedures addressing the baseline configuration of the information system
- procedures addressing configuration settings for the information system
- configuration management plan
- enterprise architecture documentation
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- security configuration checklists
- evidence supporting approved deviations from established configuration settings

- system audit records
- change control records
- other relevant documents or records

#### Who to Talk to:

- employees with configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

#### Perform Test On:

- processes for managing baseline configurations
- processes for managing configuration settings
- automated mechanisms supporting configuration control of the baseline configuration
- automated mechanisms that implement, monitor, and/or control information system configuration settings
- automated mechanisms that identify and/or document deviations from established configuration settings

### 3.4.3 Track, review, approve/disapprove, and audit changes to information systems.

Are changes to the system authorized by company management and documented?

Yes No Partially Does Not Apply Alternative Approach

Are configuration-managed changes to the system audited by company personnel?

Yes No Partially Does Not Apply Alternative Approach

Are changes tracked and documented in an approved IT service management system (ITSM) or equivalent tracking service?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Changes to information systems include modifications to hardware, software, or firmware components and configuration settings. Companies ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand company security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with facilities/processes.

Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

Changes to information systems should be reviewed and approved by company management prior to implementation.

#### Where to Look:

- configuration management policy
- procedures addressing information system configuration change control
- configuration management plan
- information system architecture and configuration documentation
- security plan
- change control records
- information system audit records change control audit and review reports
- agenda /minutes from configuration change control oversight meetings
- other relevant documents or records

#### Who to Talk to:

- employees with configuration change control responsibilities
- employees with information security responsibilities
- system/network administrators
- members of change control board or similar

#### Perform Test On:

- processes for configuration change control
- automated mechanisms that implement configuration change control

### 3.4.4 Analyze the security impact of changes prior to implementation.

Are changes that affect system security requirements tested prior to implementation?

Yes No Partially Does Not Apply Alternative Approach

Is testing the effectiveness of the changes performed?

Yes No Partially Does Not Apply Alternative Approach

Are only those changes that continue to meet compliance requirements approved and implemented?

Yes No Partially Does Not Apply Alternative Approach

Are configuration changes tested, validated, and documented before installing them on the operational system?

Yes No Partially Does Not Apply Alternative Approach

Has testing been ensured to not interfere with system operations?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Employees with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/ technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand requirement implementation and how specific changes might affect the requirements. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security requirements are required. Security impact analyses are scaled in accordance with the security categories of the information systems.

#### Where to Look:

- configuration management policy
- procedures addressing security impact analysis for changes to the information system
- configuration management plan
- security impact analysis documentation
- analysis tools and associated outputs
- change control records
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with responsibility for conducting security impact analysis
- employees with information security responsibilities
- system/network administrators

#### Perform Test On:

- processes for security impact analysis

### 3.4.5 *Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.*

Are only employees who are approved to make physical or logical changes on systems allowed to do so?

Yes No Partially Does Not Apply Alternative Approach

Are authorized personnel approved and documented by the service owner and IT security?

Yes No Partially Does Not Apply Alternative Approach

Does all change documentation include the name of the authorized employee making the change?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Companies should permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications.

Companies should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

#### **Where to Look:**

- configuration management policy
- procedures addressing access restrictions for changes to the information system
- configuration management plan
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- logical access approvals
- physical access approvals
- access credentials
- change control records
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with logical access control responsibilities
- employees with physical access control responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- processes for managing access restrictions to change
- automated mechanisms supporting/ implementing/enforcing access restrictions associated with changes to the information system



### 3.4.6 *Employ the principle of least functionality by configuring the information system to provide only essential capabilities.*

Is the information system configured to exclude any function not needed in the operational environment?

Yes No Partially Does Not Apply Alternative Approach

Does it deliver one function per system, where practical?

Yes No Partially Does Not Apply Alternative Approach

Does the system employ processing components that have minimal functionality and data storage (e.g., diskless nodes, thin client technologies)?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, companies should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., VoIP, Instant Messaging, auto-execute, and file sharing).

The deployment of information system components with reduced/minimal functionality reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber-attacks. It is good practice to block ports or protocols that are not needed in the operational environment. For example, if you do not need or use VoIP, don't allow it.

#### **Where to Look:**

- configuration management policy
- configuration management plan
- procedures addressing least functionality in the information system
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- security configuration checklists
- other relevant documents or records

#### **Who to Talk to:**

- employees with security configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- processes prohibiting or restricting functions, ports, protocols, and/or services
- automated mechanisms implementing restrictions or prohibition of functions, ports, protocols, and/or services

### 3.4.7 *Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.*

Are only those ports and protocols necessary to provide the service of the information system configured for that system?

Yes No Partially Does Not Apply Alternative Approach

Are only applications and services that are needed for the function of the system configured and enabled?

Yes No Partially Does Not Apply Alternative Approach

Are systems services reviewed to determine what is essential for the function of that system?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, companies should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., VoIP, Instant Messaging, auto-execute, and file sharing).

Companies should consider disabling unused or unnecessary physical and logical ports/ protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Companies can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

#### **Where to Look:**

- configuration management policy

- procedures addressing least functionality in the information system
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- specifications for preventing software program execution
- security configuration checklists
- documented reviews of functions, ports, protocols, and/or services
- change control records
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with responsibilities for reviewing functions, ports, protocols, and services on the information system
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- processes for reviewing/disabling non-secure functions, ports, protocols, and/or services
- automated mechanisms implementing review and disabling of non-secure functions, ports, protocols, and/or services
- processes preventing program execution on the information system
- processes for software program usage and restrictions
- automated mechanisms preventing program execution on the information system
- automated mechanisms supporting and/or implementing software program usage and restrictions

### 3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting policy to allow the execution of authorized software.

Is the information system configured to only allow authorized software to run?

Yes No Partially Does Not Apply Alternative Approach

Is the system configured to disallow running unauthorized software?

Yes No Partially Does Not Apply Alternative Approach

Is there a defined list of software programs authorized to execute on the system?

Yes No Partially Does Not Apply Alternative Approach

Is the authorization policy a deny-all, permit by exception for software allowed to execute on the system?

Yes No Partially Does Not Apply Alternative Approach

Is it reviewed at least annually?

Yes No Partially Does Not Apply Alternative Approach

Are automated mechanisms used to prevent program execution in accordance with defined lists (e.g., white listing)?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The requirements for allowing or disallowing the running of software may include (but not be limited to) the use of firewalls to restrict port access and user operational controls.

The process used to identify software programs that are authorized to execute on company information systems is commonly referred to as whitelisting.

In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.

The process used to identify software programs that are not authorized to execute on company information systems is commonly referred to as blacklisting. Organizations can implement blacklisting instead of whitelisting (the stronger of

the two policies) is the preferred approach for restricting software program execution.

Policies can also be used to prevent certain types of software from being run on the company's system (e.g., games). Enforcement of these types of policies should be checked by periodic audit. This may provide a simpler approach to meeting this requirement for some companies.

#### Where to Look:

- configuration management policy
- procedures addressing least functionality in the information system
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of software programs not authorized to execute on the information system
- list of software programs authorized to execute on the information system
- security configuration checklists
- review and update records associated with list of unauthorized software programs
- review and update records associated with list of authorized software programs
- change control records
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with responsibilities for identifying software not authorized to execute on the information system
- employees with responsibilities for identifying software authorized to execute on the information system
- employees with information security responsibilities
  - system/network administrators

#### Perform Test On:

- process for identifying, reviewing, and updating programs not authorized to execute on the information system

- process for identifying, reviewing, and updating programs authorized to execute on the information system
- process for implementing blacklisting automated mechanisms supporting and/or implementing blacklisting
- process for implementing whitelisting automated mechanisms supporting and/or implementing whitelisting

### 3.4.9 Control and monitor user-installed software.

Are user controls in place to prohibit the installation of unauthorized software?

Yes No Partially Does Not Apply Alternative Approach

Is all software in use on the information systems approved?

Yes No Partially Does Not Apply Alternative Approach

Does the company follow good practices which require that user-installed software execute in confined physical or virtual machine environment with limited privileges?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Approaches to meeting this requirement to control and monitor software installed by users can include policies and procedures. Policies should fully describe what is allowed and procedures should be in place to check that the policy is not violated.

Companies should identify software that may be of greater concern regarding origin or potential for containing malicious code. This requirement is necessary to protect the overall system processing CUI; it is not about software used to actually process CUI.

#### Where to Look:

- configuration management policy
- procedures addressing user installed software
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- employees with responsibilities for governing user-installed software
- employees operating, using, and/or maintaining the information system
- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- processes governing user-installed software on the information system
- automated mechanisms for alerting personnel/roles when unauthorized installation of software is detected

## Identification and Authentication: SP 800-171 Security Family 3.5

For most systems, identification and authentication is often the first line of defense.

Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system. Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system. Identification and authentication is a critical building block of information security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system can identify and differentiate between users. For example, access control is often based on least privilege, which refers to granting users only those accesses required to perform their duties. User accountability requires linking activities on a system to specific individuals and, therefore, requires the system to identify users. Systems recognize individuals based on the authentication data the systems receive. Authentication presents several challenges: collecting authentication data, transmitting the data securely, and knowing whether the individual who was originally authenticated is still the individual using the system. For example, a user may walk away from a terminal while still logged on, and another person may start using it. There are four means of authenticating a user's identity that can be used alone or in combination.

User identity can be authenticated based on:

- something you know – e.g., a password or Personal Identification Number (PIN),
- something you possess (a token) – e.g., an ATM card or a smart card,
- something you are (static biometric) – e.g., fingerprint, retina, face, ear, DNA, and/or
- something you do (dynamic biometrics) – e.g., voice pattern, handwriting, typing rhythm.

While it may appear that any of these individual methods could provide strong authentication, there are problems associated with each. If an individual wanted to impersonate someone else on a system, they could guess or learn another user's password, or steal or fabricate tokens. Each method also has drawbacks for legitimate users and system administrators: users forget passwords and may lose tokens, and administrative overhead for keeping track of identification and authorization data and tokens can be substantial. Biometric systems have significant technical, user acceptance, and cost problems as well. Examples of identification and authentication requirements include: device identification and authentication, identifier management, authenticator management, authenticator feedback, and re-authentication. Companies should identify system users, processes acting on behalf of users, or devices and authenticate or verify the identities of those users, processes, or devices, as a prerequisite to allowing access to company systems.

The following security requirements fall under the Identification and Authentication family.

### 3.5.1 Identify information system users, processes acting on behalf of users, or devices.

Does the system make use of company-assigned accounts for unique access by individuals?

Yes No Partially Does Not Apply Alternative Approach

If service accounts are necessary for device or process authentication, are the accounts created by the central identity management team and assigned to a member of the team using the account (separation of duties)?

Yes No Partially Does Not Apply Alternative Approach

Are company and service accounts managed centrally and deleted automatically when an individual leaves the company?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Identification of users is a prerequisite for granting access to resources within the system. It prevents unauthorized individuals or processes from entering the system. Identification and authentication of users is the basis for many types of access control and user accountability. If this security requirement is not implemented correctly it will impact the remaining Identification and Authentication security requirements.

#### Where to Look:

- identification and authentication policy
- procedures addressing user identification and authentication
- procedures addressing authenticator management
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of information system accounts
- list of information system authenticator types
- change-control records associated with managing information system authenticators
- other relevant documents or records

#### Who to Talk to:

- employees with information system operations responsibilities
- employees with information security responsibilities
- employees with authenticator management responsibilities
- system/network administrators
- employees with account management responsibilities
- system developers

#### Perform Test On:

- processes for uniquely identifying and authenticating users
- automated mechanisms supporting and/or implementing identification and authentication capability
- automated mechanisms supporting and/or implementing authenticator management capability

### 3.5.2 *Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to company information systems.*

Are the accounts in use assigned and managed by the company's central identity management system?

Yes No Partially Does Not Apply Alternative Approach

Are accounts provisioned as part of the established account creation process?

Yes No Partially Does Not Apply Alternative Approach

Are accounts uniquely assigned to new employees, contractors, or subcontractors upon hire?

Yes No Partially Does Not Apply Alternative Approach

Are initial passwords randomly generated strings provided via a password reset mechanism to each employee?

Yes No Partially Does Not Apply Alternative Approach

Is the password reset upon first use?

Yes No Partially Does Not Apply Alternative Approach

Do all passwords follow best practice of at least 12 characters, and require a mix of upper and lower case letters, numbers, and special characters?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

While passwords are commonly used for authentication. There are other more effective methods that can be employed. User identity can be authenticated based on:

- Something the user knows, this may include a password or Personal Identification Number (PIN),
- something the user possesses, a type of token such as an ATM card or a smart card,
- something the user is based on a static biometric such as a fingerprint, retina, face, ear, DNA,
- something the user does based on a dynamic biometric such as a voice pattern, handwriting, or typing rhythm.

#### **Where to Look:**

- identification and authentication policy
- procedures addressing user identification and

authentication

- procedures addressing authenticator management
- list of information system authenticator types
- change control records associated with managing information system authenticators
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of information system accounts
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system operations responsibilities
- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- employees with account management responsibilities
- system developers

#### **Perform Test On:**

- processes for uniquely identifying and authenticating users
- automated mechanisms supporting and/or implementing identification and authentication capability
- automated mechanisms supporting and/or implementing authenticator management capability



### 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Does the system uniquely identify and authenticate users?

Yes No Partially Does Not Apply Alternative Approach

Is multifactor authentication used for local access to privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Is multifactor authentication used for network access to privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Is multifactor authentication used for network access to non-privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

NIST SP 800-171 defines a “privileged user” as “a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.”

For example, if users’ computer accounts are “administrator accounts” or have “limited administrative rights” only on their computers, are they considered a “privileged account” requiring multifactor authentication at the “local access level”?

Since, in this case, the “ordinary users” are authorized to perform the function, they are not considered privileged users.

Multifactor authentication (MFA) to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a one-time password generating device like a fob, smart-card, or a mobile app on a smart-phone); and something you are (e.g., biometric like a fingerprint or iris). The traditional authentication method uses a single factor, typically a password, while multifactor authentication requires that a second factor also be used such as a PIN sent via a text message (using something you have – the cell phone) or something you are (fingerprint).

Local Access means access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Network Access means access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, internet).

1. For a NON-PRIVILEGED user, using a standalone computer (e.g., a laptop computer), with no network access, the access can be via single factor authentication (SFA); MFA is not required. However, if used to connect to a LAN, the network access must be MFA. Typically, organizational desktops are used for network access and so the user must use MFA to access their network account.
2. For a PRIVILEGED user, even local access requires MFA.

MFA is not required to access a mobile device (e.g., smart phones) even if they contain covered defense information, as there is a separate requirement in NIST SP 800-171 (3.1.19) to encrypt CUI on mobile devices and mobile computing platforms, and typically mobile devices do not support MFA in order to access the device. However, if the mobile device is used to access a Covered Contractor Information System, then the system must provide the capability for MFA for access by the device, and which would be entered via the device (e.g., use of a one-time password (OTP) device and a password).

*An example: Access to the Army project data requires use of institutional multifactor authentication services. Multifactor authentication to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a One-Time Password generating device like a fob, smart-card, or a mobile app on a smart- phone); and something you are (e.g., a biometric like a fingerprint or iris). New employees assigned to the Army project receive their account and instructions for creating a password from HR during the hiring process. New employees receive notification of their account via registered email with an activation link to set their initial password. Passwords may be reset by contacting the service desk and providing proof of identity, or using the online reset service using pre-defined challenge and response questions. Default passwords for information systems are changed before they are introduced to the network. Passwords are stored centrally in company managed authentication systems (and hashed using hashing algorithms). Encrypted transmission of passwords is required.*

**Where to Look:**

- identification and authentication policy
- procedures addressing user identification and authentication
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of information system accounts
- other relevant documents or records

**Who to Talk to:**

- employees with information system operations responsibilities
- employees with account management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

**Perform Test On:**

- automated mechanisms supporting and/ or implementing multifactor authentication capability

### 3.5.4 *Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.*

Are only anti-replay authentication mechanisms used?

Yes No Partially Does Not Apply Alternative Approach

Are defined replay-resistant authentication mechanisms used for network access to privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Are defined replay-resistant authentication mechanisms used for network access to non-privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

A replay attack may enable an unauthorized user to gain access. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack. An authentication process resists replay attacks (if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.)

The authentication front-end technologies may include, for example, shibboleth, SSH, Microsoft remote desktop protocol, and SSL VPN. Backend authentication mechanisms in use may include, for example, Kerberos and Active Directory.

Per NIST SP 800-53, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, upon which NIST SP 800-171 is based (and references if additional information is required), “authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.”

A nonce is a randomly generated value used to defeat “playback” attacks in communication protocols. One party randomly generates a nonce and sends it to the other party. The receiver encrypts it using the agreed upon secret key and returns it to the sender. Because the sender randomly generated the nonce, this defeats playback attacks because the

replayer cannot know in advance the nonce the sender will generate. The receiver denies connections that do not have the correctly encrypted nonce.

#### **Where to Look:**

- identification and authentication policy
- procedures addressing user identification and authentication
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of privileged information system accounts
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system operations responsibilities
- employees with account management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### **Perform Test On:**

- automated mechanisms supporting and/or implementing identification and authentication capability
- automated mechanisms supporting and/or implementing replay resistant authentication mechanisms

### 3.5.5 Prevent reuse of identifiers for a defined period.

Are the accounts in use assigned and managed by the company's central identity management system?

Yes No Partially Does Not Apply Alternative Approach

Are accounts provisioned as part of the established account creation process?

Yes No Partially Does Not Apply Alternative Approach

Are accounts uniquely assigned to employees, contractors, and subcontractors?

Yes No Partially Does Not Apply Alternative Approach

Are account identifiers reused?

Yes No Partially Does Not Apply Alternative Approach

Are user account names different than email user accounts?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Prohibiting the use of information systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, this makes it more difficult for adversaries to guess user identifiers on company information system.

#### Where to Look:

- identification and authentication policy
- procedures addressing identifier management
- procedures addressing account management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- list of information system accounts
- list of identifiers generated from physical access control devices
- other relevant documents or records

#### Who to Talk to:

- employees with identifier management responsibilities

- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- automated mechanisms supporting and/or implementing identifier management

### 3.5.6 *Disable identifiers after a defined period of inactivity.*

Are user accounts or identifiers monitored for inactivity?

Yes No Partially Does Not Apply Alternative Approach

Are user or device identifiers disabled after a period of inactivity (e.g., 30 days)?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Common device identifiers include, for example, media access control (MAC), internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities use account names provided. This requirement also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems. Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

#### **Where to Look:**

- identification and authentication policy
- procedures addressing identifier management
- procedures addressing account management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- list of information system accounts
- list of identifiers generated from physical access control devices
- other relevant documents or records

#### **Who to Talk to:**

- employees with identifier management responsibilities

- employees with information security responsibilities
- system/network administrators
- system developers

#### **Perform Test On:**

- automated mechanisms supporting and/or implementing identifier management

### 3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

Does the company specify a degree of complexity, e.g., are account passwords a minimum of 12 characters and a mix of upper/lower case, numbers and special characters, including minimum requirements for each type?

Yes No Partially Does Not Apply Alternative Approach

Does the company require a change of characters when new passwords are created?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The complexity of passwords can protect against brute force attacks.

#### Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator

management

- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

#### Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

### 3.5.8 Prohibit password reuse for a specified number of generations.

Can passwords be re-used after a certain number of days or a defined number of password changes?

Yes No Partially Does Not Apply Alternative Approach

Can users re-use the same password when changing their password for at least a certain number of changes?

Yes No Partially Does Not Apply Alternative Approach

Is password reuse prohibited for a defined number of generations?

Yes No Partially Does Not Apply Alternative Approach

Are passwords unique to the organization's systems and not re-used on external information systems?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The reuse of passwords can greatly diminished the effectiveness of authentication security requirements on the system. While many users may find it convenient to reuse the same password on various systems, this practice can increase the risk of a security incident.

#### Where to Look:

- identification and authentication policy
- password policy procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

#### Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

### 3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

Do new employees receive an account and instructions for creating a password during the hiring process?

Yes No Partially Does Not Apply Alternative Approach

Do new employees receive notification of their account, and are they required to reset their initial passwords?

Yes No Partially Does Not Apply Alternative Approach

Are temporary password activation links sent to validated employees should they require a password reset or change?

Yes No Partially Does Not Apply Alternative Approach

Are temporary passwords only good to allow for a password reset?

Yes No Partially Does Not Apply Alternative Approach

Does the system enforce immediate password change after logon when a temporary password is issued, e.g., lost or forgotten password?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This is the lost or forgotten password situation. The administrator issues a new password where the user can logon and the system will require the user to change the temporary password used to logon.

#### Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan

- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

#### Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability



### 3.5.10 Store and transmit only encrypted representation of passwords.

Are passwords prevented from being stored in reversible encryption form in any company systems?

Yes No Partially Does Not Apply Alternative Approach

Are passwords stored as one-way hashes constructed from passwords?

Yes No Partially Does Not Apply Alternative Approach

Does the company follow the best practice of “salting” hashed passwords?

Yes No Partially Does Not Apply Alternative Approach

Are passwords encrypted in storage and in transmission?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional information:**

“Password hashing” performs a one-way transformation on a password, turning the password into another string, called the hashed password. “One-way” means that it is practically impossible to go the other way, i.e., to turn the hashed password back into the original password.

In cryptography, a salt is random data that is used as an additional input to a one-way function that “hashes” a password or passphrase. The primary function of salts is to defend against dictionary attacks or against a pre-computed rainbow table attack. A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time, additional safeguards developed to protect a user’s password against being read from the system. A new salt is randomly generated for each password and never re-used.

#### **Where to Look:**

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

#### **Who to Talk to:**

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

#### **Perform Test On:**

- automated mechanisms supporting and/or implementing password-based authenticator management capability

### 3.5.11 Obscure feedback of authentication information.

Do the authentication mechanisms obscure feedback of authentication information during the authentication process?

Yes No Partially Does Not Apply Alternative Approach

Do the authentication mechanisms not return any system specific information such as “wrong password” or “wrong username”?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement seeks to prevent an observer from viewing authentication information, such as a password, while it is being entered. One technique to obscure feedback is to have dots appear in the password window while it is being typed instead of the actual characters being entered.

The most basic feedback control is never informing the user in an error message what part of the of the authentication transaction failed. In the case of shibboleth, for example, the error message is generic regardless of whether the userid was mistyped, the password was wrong, or (in the case of MFA) there was a problem with the MFA credential provided — the failure simply says that the credentials were invalid. Likewise, unsuccessful authentications at the Kerberos KDCs don’t distinguish between the “principal not found” and the “invalid key” case. LDAP-based authentication interfaces only return a “failure to bind” message from both the main LDAPs and the AD.

#### Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

#### Who to Talk to:

- employees with authenticator management

responsibilities

- employees with information security responsibilities
- system/network administrators
- system developers

#### Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

### **Incident Response: SP 800-171 Security Family 3.6**

Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be lessened by having standard operating procedures that can be followed in the event of an incident. For example, frequently occurring events like mistakenly deleting a file can usually be repaired through restoration from the backup file. More severe threat events, such as outages caused by natural disasters, are normally addressed in a company's contingency plan. Threat events can also result from a virus, other malicious code, or a system intruder (either an insider or an outsider). They can more generally refer to those incidents that could result in severe damage without a technical expert response. An example of a threat event that would require an immediate technical response would be an organization experiencing a denial-of service attack. This kind of attack would require swift action on the part of the incident response team to reduce the affect the attack will have on the organization. The definition of a threat event is somewhat flexible and may vary by company and computing environment. Although the threats that hackers and malicious code pose to systems and networks are well known, the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the internet), such as break-ins and service disruptions, have harmed many companies' computing capabilities. When initially confronted with such incidents, most companies respond in an ad hoc manner. However, recurrence of similar incidents can make it cost-beneficial to develop a standard capability for quick discovery of and response to such events. This is especially true since incidents can often "spread" when left unchecked, thus escalating the damage and seriously harming an organization. Incident handling is closely related to contingency planning. An incident handling capability may be viewed as a component of contingency planning because it allows for the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning specifically that responds to malicious technical threats. Examples of incident response requirements include: incident response training, incident response testing, incident handling, incident monitoring, and incident reporting. Companies should establish an operational incident handling capability for company systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and track, document, and report incidents to company management and/or authorities.

The following security requirements fall under the Incidence Response family.

**3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.**

Is there a company incident response policy which specifically outlines requirements for handling of incidents involving CUI?

Yes No Partially Does Not Apply Alternative Approach

Is an incident handling capability implemented for security incidents that include preparation, detection and analysis, containment, eradication, and recovery?

Yes No Partially Does Not Apply Alternative Approach

**Additional Information**

Organizations recognize that incident response capability is dependent on the capabilities of company information systems and the business processes being supported by those systems. Companies should consider incident response as part of the definition, design, and development of business processes and information systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many company entities including, for example, business owners, information system owners, authorizing officials, human resources, physical and personnel security offices, legal departments, operations personnel, and purchasing/procurement offices.

**Where to Look:**

- incident response policy
- procedures addressing incident response training
- contingency planning policy
- procedures addressing incident handling
- procedures addressing incident monitoring
- procedures addressing incident reporting
- incident response records and documentation
- incident response plan

- contingency plan
- incident response training curriculum
- incident response training materials
- security plan
- incident response training records
- incident reporting records and documentation
- other relevant documents or records

**Who to Talk to:**

- employees with incident response training and operational responsibilities
- employees with incident handling responsibilities
- employees with incident monitoring responsibilities
- employees with contingency planning responsibilities
- employees with incident reporting responsibilities
- personnel who have/should have reported incidents
- personnel to whom incident information is to be reported
- employees with incident response assistance and support responsibilities
- employees with access to incident response support and assistance capability
- employees with information security responsibilities

**Perform Test On:**

- incident handling capability for the company
- automated mechanisms supporting and/or implementing tracking and documenting of system security incidents
- processes for incident reporting
- automated mechanisms supporting and/or implementing incident reporting
- processes for incident response assistance
- automated mechanisms supporting and/or implementing incident response assistance

### 3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

Is there a company incident response policy which specifically outlines requirements for tracking and reporting of incidents involving CUI to appropriate officials?

Yes No Partially Does Not Apply Alternative Approach

Is cybersecurity incident information promptly reported to company management and authorities?

Yes No Partially Does Not Apply Alternative Approach

Are security incidents related to industrial control systems security incidents promptly reported to company management and authorities?

Yes No Partially Does Not Apply Alternative Approach

Are employees required to report suspected security incidents to the company's incident response authority within a defined time-period?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The intent of this requirement is to address both specific incident reporting requirements within a company and incident reporting requirements that are external to the company. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, directives, regulations, policies, standards, and guidance.

#### Where to Look:

- incident response policy
- procedures addressing incident response training
- incident response training curriculum
- incident response training materials
- procedures addressing incident response assistance
- contingency planning policy
- procedures addressing incident handling
- procedures addressing incident monitoring
- incident response records and documentation
- procedures addressing incident reporting

- incident reporting records and documentation
- contingency plan
- security plan
- incident response plan
- incident response training records
- other relevant documents or records

#### Who to Talk to:

- employees with incident response training and operational responsibilities
- employees with information security responsibilities
- employees with incident handling responsibilities
- employees with contingency planning responsibilities
- employees with incident monitoring responsibilities
- employees with incident reporting responsibilities
- personnel who have/should have reported incidents
- personnel (authorities) to whom incident information is to be reported
- personnel with incident response assistance and support responsibilities
- employees with access to incident response support and assistance capability
- employees with information security responsibilities

#### Perform Test On:

- incident handling capability for the organization
- incident monitoring capability for the organization
- automated mechanisms supporting and/or implementing tracking and documenting of system security incidents
- processes for incident reporting
- automated mechanisms supporting and/or implementing incident reporting
- processes for incident response assistance

- automated mechanisms supporting and/or implementing incident response assistance

### 3.6.3 Test the organization incident response capability.

Is there a company incident response policy?

Yes No Partially Does Not Apply Alternative Approach

Does it outline requirements for regular testing and reviews/improvements to incident response capabilities?

Yes No Partially Does Not Apply Alternative Approach

Does the company test its incident response capabilities?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Companies test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercise. Incident response testing can also include a determination of the effects on company operations (e.g., reduction in production capabilities), company assets, and individuals due to incident response.

#### Where to Look:

- incident response policy
- contingency planning policy
- procedures addressing incident response testing
- procedures addressing contingency plan testing
- incident response testing material
- incident response testing results
- incident response testing plan
- incident response testing documentation
- business continuity plans
- disaster recovery plans
- continuity of operations plans
- crisis communications plan
- critical infrastructure plans
- occupant emergency plan
- incident response plan
- contingency plan

- security plan
- other relevant documents or records

#### Who to Talk to:

- employees with incident response testing responsibilities
- employees with responsibilities for testing company plans related to incident response testing
- employees with information security responsibilities

### **Maintenance: SP 800-171 Security Family 3.7**

To keep systems in good working order and to minimize risks from hardware and software failures, it is important that companies establish procedures for systems maintenance. There are many ways a company can address these maintenance requirements. Controlled maintenance of a system deals with maintenance that is scheduled and performed in accordance with the manufacturer's specifications. Maintenance performed outside of a scheduled cycle, known as corrective maintenance, occurs when a system fails or generates an error condition that must be corrected to return the system to operational conditions. Maintenance can be performed locally or non-locally. Nonlocal maintenance is any maintenance or diagnostics performed by individuals communicating through a network either internally or externally (e.g., the internet). Examples of maintenance requirements include: controlled maintenance, maintenance tools, nonlocal maintenance, maintenance personnel, and timely maintenance. Companies should perform periodic and timely maintenance on company systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

The following security requirements fall under the Maintenance family.



### 3.7.1 Perform maintenance on organization information systems.

Are IT system maintenance tools (e.g., tools used for diagnostics, scanner and patching tools) managed?

Yes No Partially Does Not Apply Alternative Approach

Is there a list of approved tools and their access and location is controlled?

Yes No Partially Does Not Apply Alternative Approach

Are all systems, devices, and supporting systems for the company maintained per manufacturer recommendations or company defined schedules?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform maintenance on the information system?

Yes No Partially Does Not Apply Alternative Approach

Does company management approve maintenance activities?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

In general, system maintenance requirements tend to support the security objective of availability. However, improper system maintenance or a failure to perform maintenance can result in the unauthorized disclosure of CUI, thus compromising confidentiality of that information.

This requirement refers to the maintenance of company IT systems.

#### Where to Look:

- information system maintenance policy
- procedures addressing controlled information system maintenance
- maintenance records
- manufacturer/vendor maintenance specifications
- equipment sanitization records
- media sanitization records
- procedures addressing information system maintenance tools
- maintenance tool inspection records
- information system maintenance tools and associated documentation
- other relevant documents or records

#### Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities
- employees responsible for media sanitization
- system/network administrators

#### Perform Test On:

- processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
- processes for sanitizing information system components
- automated mechanisms supporting and/or implementing controlled maintenance
- automated mechanisms implementing sanitization of information system components
- processes for approving, controlling, and monitoring maintenance tools
- automated mechanisms supporting and/or implementing approval, control, and/or monitoring of maintenance tools
- processes for inspecting maintenance tools
- automated mechanisms supporting and/or implementing inspection of maintenance tools
- process for inspecting media for malicious code
- automated mechanisms supporting and/or implementing inspection of media used for maintenance

### 3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Are controls in place that limit the tools, techniques, mechanisms, and employees used to maintain information systems, devices, and supporting systems?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement seeks to manage issues that can arise from the misuse of tools, techniques, and mechanisms that are used for IT system maintenance. Diagnostic tools and software can introduce malware into company systems if not managed properly. Employees with IT maintenance responsibilities can behave in a malicious manner if not supervised and managed effectively.

Controls may include lists of authorized tools, authorized employees, and authorized techniques and mechanisms. Any such maintenance must occur within the context of other information systems controls in place.

#### Where to Look:

- information system maintenance policy
- procedures addressing controlled information system maintenance
- procedures addressing information system maintenance tools
- information system maintenance tools and associated documentation
- maintenance tool inspection records
- maintenance records
- manufacturer/vendor maintenance specifications
- equipment sanitization records
- media sanitization records
- other relevant documents or records

#### Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities

- employees responsible for media sanitization system/network administrators

#### Perform Test On:

- processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
- processes for sanitizing information system components automated mechanisms supporting and/or implementing controlled maintenance
- automated mechanisms implementing sanitization of information system components
- processes for approving, controlling, and monitoring maintenance tools
- automated mechanisms supporting and/or implementing approval, control, and/or monitoring of maintenance tools
- processes for inspecting maintenance tools
- automated mechanisms supporting and/or implementing inspection of maintenance tools
- process for inspecting media for malicious code
- automated mechanisms supporting and/or implementing inspection of media used for maintenance

### 3.7.3 *Ensure equipment removed for off-site maintenance is sanitized of any CUI.*

Is there a company media sanitization policy?

Yes No Partially Does Not Apply Alternative Approach

Are media that are removed from the premises for maintenance, repair, or disposal sanitized per the company's media sanitization policies?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This requirement addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes: date and time of maintenance, name of individuals or group performing the maintenance, name of escort (if necessary), a description of the maintenance performed, and information system components/equipment removed or replaced (including identification numbers, if applicable). Companies should consider supply chain issues associated with replacement components for information systems.

#### **Where to Look:**

- media sanitization policy
- information system maintenance policy
- procedures addressing controlled information system maintenance
- maintenance records
- manufacturer/vendor maintenance specifications
- equipment sanitization records
- media sanitization records
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system maintenance responsibilities
- employees with information security responsibilities

- employees responsible for media sanitization
- system/network administrators

#### **Perform Test On:**

- processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
- processes for sanitizing information system components
- automated mechanisms supporting and/or implementing controlled maintenance
- automated mechanisms implementing sanitization of information system components

### 3.7.4 *Check media containing diagnostics and test programs for malicious code before the media are used in the information system.*

Are media that are provided by authorized maintenance personnel (and not normal systems administrators/owners) for troubleshooting, diagnostics, or other maintenance run through an anti-virus/anti-malware/anti-spyware program prior to use in the company's information system?

Yes No Partially Does Not Apply Alternative Approach

Are the results of the scans documented in the maintenance logs?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Malicious code is often introduced to a system by media used for diagnostic or testing purposes. All media provided by authorized maintenance personnel should be scanned for malware.

#### **Where to Look:**

- information system maintenance policy
- procedures addressing information system maintenance tools
- information system maintenance tools and associated documentation
- maintenance records
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system maintenance responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- process for inspecting media for malicious code
- automated mechanisms supporting and/or implementing inspection of media used for maintenance

### 3.7.5 *Require multifactor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.*

Does all remote access to a system for maintenance or diagnostics occur via an approved remote solution using multifactor authentication?

Yes No Partially Does Not Apply Alternative Approach

Does the system require multifactor authentication for remote access?

Yes No Partially Does Not Apply Alternative Approach

Are all sessions and remote connections terminated when remote maintenance is completed?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

The multifactor authentication for non-local maintenance is intended for recurring non-local maintenance by organizational personnel rather than episodic non-local maintenance by outside vendors where issuance of such credentials for one-time activities is not efficient and may not be advisable. Presuming the individual performing the repair is known and trusted, it is possible to provide for “one-time” multifactor authentication using a password and a separately provided token (e.g., PIN via text message to a cell phone).

#### **Where to Look:**

- information system maintenance policy
- procedures addressing nonlocal information system maintenance
- security plan

- system design documentation
- information system configuration settings and associated documentation
- maintenance records
- diagnostic records
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system maintenance responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- processes for managing nonlocal maintenance
- automated mechanisms implementing, supporting, and/or managing nonlocal maintenance
- automated mechanisms for strong authentication of nonlocal maintenance diagnostic sessions
- automated mechanisms for terminating nonlocal maintenance sessions and network connections

### 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

Are all activities of maintenance personnel (who do not normally have access to a system) monitored?

Yes No Partially Does Not Apply Alternative Approach

Has the company defined approved methods for supervision?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Escorting maintenance personnel while they work in company facilities can provide a level of supervision over their activities.

#### Where to Look:

- information system maintenance policy
- procedures addressing maintenance personnel

- service provider contracts service-level agreements
- list of authorized personnel
- maintenance records
- access control records
- other relevant documents or records

#### Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for authorizing and managing maintenance personnel
- automated mechanisms supporting and/or implementing authorization of maintenance personnel

### **Media Protection: SP 800-171 Security Family 3.8**

Media protection is a requirement that addresses the defense of system media, which can be described as both digital and non-digital. Examples of digital media include: diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Examples of non-digital media include paper or microfilm. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed. Media protections also include physically controlling system media and ensuring accountability, as well as restricting mobile devices capable of storing and carrying information into or outside of restricted areas. Examples of media protection requirements include: media access, media marking, media storage, media transport, and media sanitization. Companies should protect system media, both paper and digital, limit access to information on system media to authorized users, and sanitize or destroy system media before disposal or release for reuse.

The following security requirements fall under the Media Protection family.

### 3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

Have responsible parties for data in these systems documented and ensured proper authorization controls for data in media and print?

Yes No Partially Does Not Apply Alternative Approach

Are documented workflow, data access controls, and media policy enforced to ensure proper access controls?

Yes No Partially Does Not Apply Alternative Approach

Is the system media securely stored in protected areas?

Yes No Partially Does Not Apply Alternative Approach

Do only approved individuals have access to media from CUI systems?

Yes No Partially Does Not Apply Alternative Approach

Is an audit log of any media removed from these systems?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which companies provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information system. For media containing information determined by companies to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the company or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

#### Where to Look:

- information system media protection policy
- procedures addressing media access restrictions

- procedures addressing media storage
- audit records
- information system design documentation
- information system configuration settings and associated documentation
- physical and environmental protection plan
- access control policy and procedures
- physical and environmental protection policy and procedures
- media storage facilities access control records
- security plan
- information system media designated controlled areas
- other relevant documents or records

#### Who to Talk to:

- employees with information system media protection responsibilities
- employees with information system media storage responsibilities
- employees with information security responsibilities
- system/network administrators

#### Perform Test On:

- processes for restricting information media
- automated mechanisms supporting and/or implementing media access restrictions
- processes for storing information media
- automated mechanisms supporting and/or implementing secure media storage/media protection
- processes for media sanitization
- automated mechanisms supporting and/or implementing media sanitization



### 3.8.2 *Limit access to CUI on information system media to authorized users.*

Are all CUI systems managed under least access rules?

Yes No Partially Does Not Apply Alternative Approach

Does the company limit CUI media access to authorized users?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which companies provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by companies to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the company or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

#### **Where to Look:**

- information system media protection policy
- procedures addressing media access restrictions
- access control policy and procedures
- procedures addressing media storage
- media sanitization and disposal plan
- media sanitization policy
- media sanitization records
- audit records
- information system design documentation
- information system configuration settings and associated documentation
- security plan
- information system media designated controlled areas

- physical and environmental protection policy and procedures
- media storage facilities access control records
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system media protection responsibilities
- employees with information system media protection and storage responsibilities
- employees with media sanitization responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- processes for restricting information media
- automated mechanisms supporting and/or implementing media access restrictions
- processes for storing information media
- automated mechanisms supporting and/or implementing secure media storage/media protection
- processes for media sanitization
- automated mechanisms supporting and/or implementing media sanitization

### 3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.

Is all managed data storage erased, encrypted, or destroyed using mechanisms to ensure that no usable data is retrievable?

Yes No Partially Does Not Apply Alternative Approach

Is system digital and non-digital media sanitized before disposal or release for reuse?

Yes No Partially Does Not Apply Alternative Approach

Are all CUI data on media encrypted or physically locked prior to transport outside of the company's secure locations?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement applies to all information system media, both digital and nondigital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Companies should determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Companies may use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.

NIST SP 800-88 "Guidelines for Media Sanitization" provides useful information that will assist companies in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>.

#### Where to Look:

- information system media protection policy
- procedures addressing media access restrictions
- procedures addressing media storage
- procedures addressing media sanitization and disposal
- media sanitization policy
- media sanitization records
- audit records
- information system design documentation
- information system configuration settings and associated documentation
- security plan
- information system media designated controlled areas
- access control policy and procedures
- physical and environmental protection policy and procedures
- media storage facilities access control records
- other relevant documents or records

#### Who to Talk to:

- employees with information system media protection responsibilities
- employees with information security responsibilities
- employees with media sanitization responsibilities
- employees with information system media protection and storage responsibilities
- system/network administrators

#### Perform Test On:

- processes for restricting information media
- automated mechanisms supporting and/or implementing media access restrictions
- processes for storing information media
- automated mechanisms supporting and/or implementing secure media storage/media protection
- processes for media sanitization
- automated mechanisms supporting and/or implementing media sanitization

### 3.8.4 Mark media with necessary CUI markings and distribution limitations.

Are all CUI systems identified with an asset control identifier, for example, does each company laptop have an asset id tag with a unique number?

Yes No Partially Does Not Apply Alternative Approach

Are removable system media and system output marked?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes regarding internal data structures within information systems. Security marking is generally not required for media containing information determined by companies to be in the public domain or to be publicly releasable. However, some companies may require markings for public information indicating that the information is publicly releasable.

This security requirement is meant to be applied by using physical controls to access physical media, but other mechanisms for logical access are acceptable. It applies to information system media, which includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. It does not include cell or smartphones.

The requirements of the DFARS clause only apply to covered defense information, i.e., information provided or developed by the contractor for DOD which is Controlled Technical Information or other information requiring protection by law, regulation, or government-wide policy. It does not apply to information provided by or developed for non-DOD organizations. Guidance on marking media, along with other materials, should be addressed separately in the contract and is derived from DOD Manual 5200.01, Volume 4, "DOD Information Security Program: Controlled Unclassified Information (CUI).

#### Where to Look:

- information system media protection policy
- procedures addressing media marking
- physical and environmental protection

policy and procedures

- security plan
- list of information system media marking security attributes
- designated controlled areas
- other relevant documents or records

#### Who to Talk to:

- employees with information system media protection and marking responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for marking information media
- automated mechanisms supporting and/or implementing media marking

### 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Do only approved individuals have access to media from CUI systems?

Yes No Partially Does Not Apply Alternative Approach

Is an audit log of any media removed from these systems?

Yes No Partially Does Not Apply Alternative Approach

Is accountability for system media maintained during transport outside controlled areas?

Yes No Partially Does Not Apply Alternative Approach

Are all CUI data on media encrypted or physically locked prior to transport outside of the company's secure locations?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement also applies to mobile devices with information storage capability (e.g., smartphones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Safeguards to protect media during transport include, for example, locked rooms, containers, and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes.

For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Companies should establish documentation requirements for activities associated with the transport of information system media in accordance

with company assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

#### Where to Look:

- information system media protection policy
- procedures addressing media storage
- physical and environmental protection policy and procedures
- access control policy and procedures
- security plan
- information system media designated controlled areas
- other relevant documents or records

#### Who to Talk to:

- employees with information system media protection and storage responsibilities
- employees with information security responsibilities
- system/network administrators

#### Perform Test On:

- processes for storing information media
- automated mechanisms supporting and/or implementing media storage/media protection

### 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Are all CUI data on media encrypted or physically locked prior to transport outside of the company?

Yes No Partially Does Not Apply Alternative Approach

Are cryptographic mechanisms used to protect digital media during transport outside of controlled areas?

Yes No Partially Does Not Apply Alternative Approach

Does removable media support physical encryption?

Yes No Partially Does Not Apply Alternative Approach

Is key vaulting utilized to ensure recoverability?

Yes No Partially Does Not Apply Alternative Approach

Are data backups encrypted on media before removal from the company's secured facility?

Yes No Partially Does Not Apply Alternative Approach

Do cryptographic mechanisms comply with FIPS 140-2?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement also applies to mobile computing and communications devices with information storage capability (e.g., notebooks/ laptop computers, personal digital assistants, cell/smart phones, digital cameras and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail).

Key vaults help safeguard cryptographic keys and secrets systems, applications, and services. By using a key vault, you can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs. Key vaults streamline the key management process and enables you to maintain control of keys that access and encrypt your data.

#### Where to Look:

- information system media protection policy
- procedures addressing media transport

- information system design documentation
- information system configuration settings and associated documentation
- information system media transport records
- audit records
- other relevant documents or records

#### Who to Talk to:

- employees with information system media transport responsibilities
- employees with information security responsibilities

#### Perform Test On:

- cryptographic mechanisms protecting information on digital media during transportation outside controlled areas

### 3.8.7 Control the use of removable media on information system components.

Is the use of writable, removable media restricted on the system?

Yes No Partially Does Not Apply Alternative Approach

Are removable media allowed?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Removable media will only be allowed if there are processes in place to control them. Removable media must be able to support physical encryption, and key vaulting must be utilized to ensure recoverability.

The use of non-digital media such as paper files should also be controlled.

#### Where to Look:

- information system media protection policy
- system use policy
- procedures addressing media usage restrictions

- security plan
- rules of behavior
- information system design documentation
- information system configuration settings and associated documentation
- audit records
- other relevant documents or records

#### Who to Talk to:

- employees with information system media use responsibilities
- employees with information security responsibilities system/network administrators

#### Perform Test On:

- processes for media use
- automated mechanisms prohibiting use of media on information systems or system components

### 3.8.8 *Prohibit the use of portable storage devices when such devices have no identifiable owner.*

Do all portable storage devices have identifiable owners?

Yes No Partially Does Not Apply Alternative Approach

Have unused removable media that contain support files been removed or disabled?

Yes No Partially Does Not Apply Alternative Approach

Are only approved portable storage devices under asset management used to store CUI data?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Only approved portable storage devices under asset management are to be used to store CUI data. Portable storage devices are small hard drives designed to hold digital data.

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

#### **Where to Look:**

- information system media protection policy
- system use policy
- procedures addressing media usage restrictions
- security plan
- rules of behavior
- information system design documentation

- information system configuration settings and associated documentation
- audit records
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system media use responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- processes for media use
- automated mechanisms prohibiting use of media on information systems or system components

### 3.8.9 *Protect the confidentiality of backup CUI at storage locations.*

Are data backups encrypted on media before removal from a secured facility?

Yes No Partially Does Not Apply Alternative Approach

Is the confidentiality and integrity of backup information protected at the storage location?

Yes No Partially Does Not Apply Alternative Approach

Are data backups encrypted on media before removal from the company's secured facility?

Yes No Partially Does Not Apply Alternative Approach

Do cryptographic mechanisms comply with FIPS 140-2?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by companies to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this requirement. Information system backups reflect the requirements in contingency plans as well as other company requirements for backing up information.

#### **Where to Look:**

- contingency planning policy
- procedures addressing information system backup
- contingency plan
- backup storage location(s)
- information system backup logs or records
- other relevant documents or records

#### **Who to Talk to:**

- employees with information system backup responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- processes for conducting information system backups

- automated mechanisms supporting and/or implementing information system backups



### **Personnel Security: SP 800-171 Security Family 3.9**

Users play a vital role in protecting a system as many important issues in information security involve users, designers, implementers, and managers. How these individuals interact with the system and the level of access they need to do their jobs can also impact the system's security posture. Almost no system can be secured without properly addressing these aspects of personnel security. Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources. A company's status and reputation can be damaged by the actions of its employees. Employees may have access to extremely sensitive, or proprietary information, the disclosure of which can destroy an organization's reputation or cripple it financially. Companies should be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated. The sensitive nature and value of company assets requires in-depth personnel security measures. Examples of personnel requirement include: personnel screening, personnel termination, personnel transfer, access agreements, and personnel sanctions. Companies should ensure that individuals occupying positions of responsibility within the company (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensure that company information and systems are protected during and after personnel actions such as terminations and transfers, and employ formal sanctions for personnel failing to comply with company security policies and procedures.

The following security requirements fall under the Personnel Security family.

### 3.9.1 Screen individuals prior to authorizing access to information systems containing CUI.

Are individuals requiring access screened before access is granted?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Companies may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

#### Where to Look:

- personnel security policy
- procedures addressing personnel screening
- procedures addressing personnel termination
- procedures addressing personnel transfer
- records of personnel transfer actions
- list of information system and facility access authorizations
- records of personnel termination actions
- list of information system accounts
- records of terminated or revoked authenticators/credentials
- records of exit
- records of screened personnel
- security plan
- other relevant documents or records

#### Who to Talk to:

- employees with personnel security responsibilities
- employees with account management responsibilities
- employees with account management responsibilities
- system/network administrators
- employees with information security responsibilities

#### Perform Test On:

- processes for personnel screening
- processes for personnel termination
- automated mechanisms supporting and/ or implementing personnel termination notifications automated mechanisms for disabling information system access/revoking authenticators
- processes for personnel transfer
- automated mechanisms supporting and/ or implementing personnel transfer notifications
- automated mechanisms for disabling information system access/revoking authenticators

### 3.9.2 *Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.*

Does the company disable information system access prior to employee termination or transfer?

Yes No Partially Does Not Apply Alternative Approach

Does the company revoke authenticators/ credentials associated with the employee upon termination or transfer within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Does the company retrieve all company information system-related property from the terminated or transferred employee within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Does the company retain access to company information and information systems formerly controlled by the terminated or transferred employee within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Does the company notify the information security office and data owner of the change in authorization within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Are electronic and physical access permissions reviewed when employees are reassigned or transferred?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This requirement applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Companies define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within companies include returning old and issuing new keys, identification cards, and building passes, closing information system accounts and establishing new accounts, changing information system access authorizations (i.e., privileges) and providing for access to official records to which employees had access at previous work locations and in previous information system accounts.

#### **Where to Look:**

- personnel security policy

- procedures addressing personnel screening
- procedures addressing personnel termination
- procedures addressing personnel transfer
- records of personnel transfer
- actions list of information system and facility access authorizations
- records of personnel termination actions
- list of information system accounts
- records of terminated or revoked authenticators/credentials
- records of exit
- records of screened personnel
- security plan
- other relevant documents or records

#### **Who to Talk to:**

- employees with personnel security responsibilities
- employees with account management responsibilities
- system/network administrators
- employees with information security responsibilities

#### **Perform Test On:**

- processes for personnel screening
- processes for personnel termination
- automated mechanisms supporting and/or implementing personnel termination notifications
- automated mechanisms for disabling information system access/revoking authenticators
- processes for personnel transfer
- automated mechanisms supporting and/or implementing personnel transfer notifications
- automated mechanisms for disabling information system access/revoking authenticators

### **Physical Protection: SP 800-171 Security Family 3.10**

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Physical and environmental requirements cover three broad areas:

1. The physical facility is typically the building, other structure, or vehicle housing the system and network components. Systems can be characterized, based upon their operating location, as static, mobile, or portable. Static systems are installed in structures at fixed locations. Mobile systems are installed in vehicles that perform the function of a structure, but not at a fixed location. Portable systems may be operated in a wide variety of locations, including buildings, vehicles, or in the open. The physical characteristics of these structures and vehicles determine the level of physical threats such as fire, roof leaks, or unauthorized access.
2. The facility's general geographic operating location determines the characteristics of natural threats, which include earthquakes and flooding; man-made threats such as burglary, civil disorders, or interception of transmissions and emanations; and damaging nearby activities, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters (e.g., radars).
3. Supporting facilities are those services (both technical and human) that maintain the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and cause physical damage to system hardware or stored data.

Examples of physical and environmental requirements include: physical access authorizations, physical access control, monitoring physical access, emergency shutoff, emergency power, emergency lighting, alternate work site, information leakage, and asset monitoring and tracking. Companies should limit physical access to systems, equipment, and the respective operating environments to authorized individuals, protect the physical plant and support infrastructure for systems, provide supporting utilities for systems, protect systems against environmental hazards, and provide appropriate environmental controls in facilities containing systems.

The following security requirements fall under the Physical Protection family.

### 3.10.1 Limit physical access to company information systems, equipment, and the respective operating environments to authorized individuals.

Has the facility/building manager designated building areas as “sensitive” and designed physical security protections (including guards, locks, cameras, card readers, etc.) to limit physical access to the area to only authorized employees?

Yes No Partially Does Not Apply Alternative Approach

Are output devices such as printers placed in areas where their use does not expose data to unauthorized individuals?

Yes No Partially Does Not Apply Alternative Approach

Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement applies to company employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forgery-proof badges, smart cards, or identification cards). This requirement only applies to areas within facilities that have not been designated as publicly accessible.

The purpose of this requirement is simply to protect the information system/equipment by limiting physical access to the information system equipment to authorized organizational personnel (e.g., employees).

#### Where to Look:

- physical and environmental protection policy
- procedures addressing physical access authorizations
- procedures addressing access control for display medium
- procedures addressing physical access monitoring
- physical access logs or records

- physical access monitoring records
- physical access log reviews
- facility layout of information system components
- actual displays from information system components
- security plan
- authorized personnel access list
- authorization credentials
- physical access list reviews
- physical access termination records and associated documentation
- other relevant documents or records

#### Who to Talk to:

- employees with physical access authorization responsibilities
- employees with physical access to information system facility
- employees with physical access control responsibilities
- employees with physical access monitoring responsibilities
- employees with incident response responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for physical access authorizations
- automated mechanisms supporting and/or implementing physical access authorizations
- processes for access control to output devices
- automated mechanisms supporting and/or implementing access control to output devices
- processes for monitoring physical access
- automated mechanisms supporting and/or implementing physical access monitoring
- automated mechanisms supporting and/or implementing reviewing of physical access logs

### 3.10.2 *Protect and monitor the physical facility and support infrastructure for those information systems.*

Has the facility/building manager reviewed the location and type of physical security in use (including guards, locks, card readers, etc.) and evaluated its suitability for the company's needs?

Yes No Partially Does Not Apply Alternative Approach

Is physical access monitored to detect and respond to physical security incidents?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Company incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

#### **Where to Look:**

- physical and environmental protection policy
- procedures addressing physical access authorizations
- procedures addressing access control for display medium
- procedures addressing physical access monitoring
- physical access logs or records
- physical access monitoring records
- physical access log reviews
- facility layout of information system components
- actual displays from information system components
- security plan
- authorized personnel access list
- authorization credentials
- physical access list reviews
- physical access termination records and associated documentation

- other relevant documents or records

#### **Who to Talk to:**

- employees with physical access authorization responsibilities
- employees with physical access to information system facility
- employees with physical access control responsibilities
- employees with physical access monitoring responsibilities
- employees with incident response responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- processes for physical access authorizations
- automated mechanisms supporting and/or implementing physical access authorizations
- processes for access control to output devices
- automated mechanisms supporting and/or implementing access control to output devices
- processes for monitoring physical access
- automated mechanisms supporting and/or implementing physical access monitoring
- automated mechanisms supporting and/or implementing reviewing of physical access logs

### 3.10.3 Escort visitors and monitor visitor activity.

Are all visitors to sensitive areas always escorted by an authorized employee?

Yes No Partially Does Not Apply Alternative Approach

Are visitors escorted and monitored as required in security policies and procedures?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Visitor access records include names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

#### Where to Look:

- physical and environmental protection policy
- procedures addressing physical access control
- security plan
- physical access control logs or records
- inventory records of physical access control devices
- information system entry and exit points
- records of key and lock combination changes
- storage locations for physical access control devices
- physical access control devices
- list of security safeguards controlling access to designated publicly accessible areas within facility
- other relevant documents or records

#### Who to Talk to:

- employees with physical access control responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for physical access control
- automated mechanisms supporting and/or implementing physical access control
- physical access control devices

### 3.10.4 Maintain audit logs of physical access.

Are logs of physical access to sensitive areas maintained per retention policies? (This includes authorized access as well as visitor access.)

Yes No Partially Does Not Apply Alternative Approach

Are visitor access records retained for as long as required by approved policy?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement applies to company employees and visitors. Individuals (employees with physical access control responsibilities, employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Companies determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within company facilities include cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.

Companies have flexibility in the types of audit logs they employ. Audit logs can be procedural, implemented by employees with physical access control responsibilities, a written log of individuals accessing the facility and when such access occurred), automated (employees with physical access control responsibilities, capturing ID provided by a smart card or badge), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both.

Components of company information systems (e.g., employees with physical access control responsibilities, workstations, terminals) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

#### Where to Look:

- physical and environmental protection policy
- procedures addressing physical access control
- security plan
- physical access control logs or records

- inventory records of physical access control devices
- information system entry and exit points
- records of key and lock combination changes
- storage locations for physical access control devices
- physical access control devices
- list of security safeguards controlling access to designated publicly accessible areas within facility
- other relevant documents or records

#### Who to Talk to:

- employees with physical access control responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for physical access control
- automated mechanisms supporting and/or implementing physical access control
- physical access control devices



### 3.10.5 Control and manage physical access devices.

Are physical access devices (such as card readers, proximity readers, and locks) maintained and operated per the manufacturer recommendations?

Yes No Partially Does Not Apply Alternative Approach

Are these devices updated with any changed access control information necessary to prevent unauthorized access?

Yes No Partially Does Not Apply Alternative Approach

Does the facility/building manager review the location and type of each physical access device and evaluate its suitability for the company's needs?

Yes No Partially Does Not Apply Alternative Approach

Are keys, combinations, and other physical access devices secured?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within company facilities include cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.

Companies have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a smart card or badge), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of company information systems (e.g., workstations, terminals) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

#### Where to Look:

- physical and environmental protection policy

- procedures addressing physical access control
- security plan
- physical access control logs or records
- inventory records of physical access control devices
- information system entry and exit points
- records of key and lock combination changes
- storage locations for physical access control devices
- physical access control devices
- list of security safeguards controlling access to designated publicly accessible areas within facility
- other relevant documents or records

#### Who to Talk to:

- employees with physical access control responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for physical access control
- automated mechanisms supporting and/or implementing physical access control
- physical access control devices

### 3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

Do all alternate sites where CUI data is stored or processed meet the same physical security requirements as the main site?

Yes No Partially Does Not Apply Alternative Approach

Does the alternate processing site provide information security measures equivalent to those of the primary site?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Companies may define different sets of security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This requirement supports the contingency planning activities of the company.

This requirement simply means that if you have alternate work sites that will be used to store, process, or transmit CUI, that the same requirements apply (i.e., there is no difference in requirements between the primary and alternate work sites), although different methods may be used to meet the requirements at the alternate site.

#### Where to Look:

- physical and environmental protection policy
- procedures addressing alternate work sites for employees
- security plan
- list of security requirements required for alternate work sites
- assessments of security requirements at alternate work sites
- other relevant documents or records

#### Who to Talk to:

- employees approving use of alternate work sites
- employees using alternate work sites
- employees assessing controls at alternate

work sites

- employees with information security responsibilities

#### Perform Test On:

- processes for security at alternate work sites
- automated mechanisms supporting alternate work sites
- security requirements employed at alternate work sites
- means of communications between personnel at alternate work sites and security personnel

### **Risk Assessment: SP 800-171 Security Family 3.11**

Companies are dependent upon information technology and associated systems. While the increasing number of information technology products used in various companies and industries can be beneficial, in some instances they may also introduce serious threats that can adversely affect a company's systems by exploiting both known and unknown vulnerabilities. The exploitation of vulnerabilities in company systems can compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Performing a risk assessment is one of four components of risk management. Risk assessments identify and prioritize risks to company operations, assets, employees, and other organizations that may result from the operation of a system. Risk assessments inform company decision makers and support risk responses by identifying: relevant threats to organizations or threats directed through organizations against other organizations, vulnerabilities both internal and external to organizations, impact (i.e., harm) to the company that may occur given the potential for threats exploiting vulnerabilities, and the likelihood that harm will occur.

Examples of risk assessment requirements include: security categorization, risk assessment, vulnerability scanning, and technical surveillance countermeasures survey. Companies should periodically assess the risk to operations (e.g., mission, functions, image, reputation), assets, and employees, which may result from the operation of company systems and the associated processing, storage, or transmission of company information.

The following security requirements fall under the Risk Assessment family.

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

Does the company have a risk management policy?

Yes No Partially Does Not Apply Alternative Approach

Have an initial and periodic risk assessments been conducted?

Yes No Partially Does Not Apply Alternative Approach

Are changes in use or infrastructure documented and assessed?

Yes No Partially Does Not Apply Alternative Approach

Is the risk assessment viewed as a living document and incorporated into the larger risk management for the system?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Risk assessments play a critical role in the development and implementation of effective information security programs and help companies address a range of security-related issues from advanced persistent threats to supply chain concerns. The results of risk assessments are used to develop specific courses of action that can provide effective response measures to the identified risks as part of a broad-based risk management process.

There is no defined requirement, methodology, or period for the assessments, nor is a report required. These are dependent on the organization, its mission, changes to its systems and environment. This is a periodic assessment of how you operate to insure you understand your risk, which can change over time. Any changes resulting from the assessment would be reflected in implementing plans of action and in the system security plan per NIST SP 800-171 requirements 3.12.2 and 3.12.4.

Additional information on conducting risk assessments can be found in NIST 800-30 Rev 1 “Guide for Conducting Risk Assessments”

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

Additional information

#### Where to Look:

- risk assessment policy
- security planning policy and procedures
- procedures addressing company assessments of risk
- security plan
- risk assessment
- risk assessment results
- risk assessment reviews
- risk assessment updates
- other relevant documents or records

#### Who to Talk to:

- employees with risk assessment responsibilities
- employees with information security responsibilities

#### Perform Test On:

- processes for risk assessment
- automated mechanisms supporting and/ or for conducting, documenting, reviewing, disseminating, and updating the risk assessment

### 3.11.2 *Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.*

Is vulnerability scanning performed?

Yes No Partially Does Not Apply Alternative Approach

Are systems periodically scanned for common and new vulnerabilities?

Yes No Partially Does Not Apply Alternative Approach

Are previously undocumented vulnerabilities risk assessed and documented?

Yes No Partially Does Not Apply Alternative Approach

Are reports regarding the scans made available to system owners and company management in a timely manner?

Yes No Partially Does Not Apply Alternative Approach

Are vulnerability scans performed on a defined frequency or randomly in accordance with company policy?

Yes No Partially Does Not Apply Alternative Approach

Is the list of scanned system vulnerabilities updated on a defined frequency or when new vulnerabilities are identified and reported?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Vulnerability scanning identifies hosts and host attributes (e.g., operating systems, applications, open ports), but it also attempts to identify vulnerabilities rather than relying on human interpretation of the scanning results. Many vulnerability scanners are equipped to accept results from network discovery and network port and service identification, which reduces the amount of work needed for vulnerability scanning.

Also, some scanners can perform their own network discovery and network port and service identification. Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy. This is done by identifying the operating systems and major software applications running on the hosts and matching them with information on known vulnerabilities stored in the scanners' vulnerability databases.

Vulnerability scanners can: check compliance with host application usage and security policies; provide information on targets for penetration testing; and provide information on how to mitigate discovered vulnerabilities.

#### **Where to Look:**

- risk assessment policy
- procedures addressing vulnerability scanning records
- risk assessment
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- list of information system components for vulnerability scanning
- personnel access authorization list
- authorization credentials
- access authorization
- security assessment report
- vulnerability scanning tools and associated configuration documentation
- vulnerability scanning results
- patch and vulnerability management records
- other relevant documents or records

#### **Who to Talk to:**

- employees with risk assessment, security control assessment and vulnerability scanning responsibilities
- employees with vulnerability scan analysis responsibilities
- employees with vulnerability remediation responsibilities
- personnel with vulnerability scanning responsibilities system/network administrators
- employees responsible for access control to the information system
- employees responsible for configuration management of the information system
- system developers
- employees with information security

responsibilities

- system/network administrators

**Perform Test On:**

- processes for vulnerability scanning, analysis, remediation, and information sharing
- automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing
- processes for vulnerability scanning
- processes for access control
- automated mechanisms supporting and/or implementing access control
- automated mechanisms/tools supporting and/ or implementing vulnerability scanning

### 3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

Do system owners and company managers upon recognition of any vulnerability provide an action plan for remediation, acceptance, avoidance, or transference of the vulnerability risk?

Yes No Partially Does Not Apply Alternative Approach

Does the plan include a reasonable time frame for implementation?

Yes No Partially Does Not Apply Alternative Approach

Are all high vulnerabilities prioritized?

Yes No Partially Does Not Apply Alternative Approach

Does the Plan of Action call out remedial security actions to mitigate risk to company operations, assets, employees, and other organizations?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to company operations and assets, employees, and other organizations based on the operation and use of information systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating information systems on behalf of the company, individuals accessing company information systems, outsourcing entities).

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle.

#### Where to Look:

- risk assessment policy
- procedures addressing vulnerability scanning
- risk assessment
- security plan
- security assessment report
- vulnerability scanning tools and associated configuration documentation
- vulnerability scanning results

- patch and vulnerability management records
- other relevant documents or records

#### Who to Talk to:

- employees with risk assessment, security requirement assessment and vulnerability scanning responsibilities
- employees with vulnerability scan analysis responsibilities
- employees with vulnerability remediation responsibilities
- employees with information security responsibilities
- system/network administrators

#### Perform Test On:

- processes for vulnerability scanning, analysis, remediation, and information sharing
- automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing

### **Security Assessment: SP 800-171 Security Family 3.12**

A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The assessment also helps determine if the implemented requirements are the most effective and cost-efficient solution for the function they are intended to serve. Assessment of the security requirements is done on a continuous basis to support a near real-time analysis of the organization's current security posture. Following a complete and thorough security requirement assessment, the company makes the decision to authorize the system to operate (for a new system) or to continue to operate. Examples of security assessment and authorization requirements include: security assessments, system interconnections, plans of action, continuous monitoring, and system security plans. Companies should periodically assess the security requirements in company systems to determine if the requirements are effective in their application, develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company systems, authorize the operation of company systems and any associated system connections, and monitor security requirements on an ongoing basis to ensure the continued effectiveness of the requirements, and document these actions in the System Security Plan.

The following security requirements fall under the Security Assessment family.



### 3.12.1 Periodically assess the security controls in company information systems to determine if the controls are effective in their application.

Has a periodic (e.g., annual) security assessment been conducted to ensure that security controls are implemented correctly and meet the security requirements?

Yes No Partially Does Not Apply Alternative Approach

Does the assessment scope include all information systems and networks, including all security requirements and procedures necessary to meet the compliance requirements of the environment?

Yes No Partially Does Not Apply Alternative Approach

Does the assessment include, but is not limited to, vulnerability scanning, penetration testing, security control testing and reviews, configuration testing and reviews, log reviews, and talking with company employees?

Yes No Partially Does Not Apply Alternative Approach

Is the assessment conducted by company employees?

Yes No Partially Does Not Apply Alternative Approach

Is the assessment conducted by an independent security auditor/consultant?

Yes No Partially Does Not Apply Alternative Approach

Is a final written assessment report and findings provided to company management after the assessment?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

To satisfy periodic (e.g., annual) assessment requirements, companies can use assessment results from the initial or ongoing information system authorizations, continuous monitoring, or system development life cycle activities.

Companies should ensure that security assessment results are current, relevant to the determination of security requirement effectiveness, and obtained with the appropriate level of assessor independence. Existing security requirement assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Companies should establish the frequency for ongoing security requirement assessments in accordance with company continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedure. Assessments should be performed at least annually. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this requirement.

The company should define for itself when requirements are assessed, which may be based on a timeframe determined by its needs and/or events, such as a change to the system or its environment.

#### Where to Look:

- security assessment and authorization policy
- procedures addressing security assessment planning
- procedures addressing security assessments
- procedures addressing plan of action
- procedures addressing continuous monitoring of information system security requirements
- procedures addressing configuration management
- plan of action
- information system monitoring records
- configuration management records
- security impact analyses
- status reports
- security plan
- security assessment report
- security assessment evidence
- plan of action
- security assessment plan
- other relevant documents or records

#### Who to Talk to:

- employees with security assessment

responsibilities

- employees with plan of action development and implementation responsibilities
- employees with continuous monitoring responsibilities
- employees with information security responsibilities

**Perform Test On:**

- automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting
- automated mechanisms for developing, implementing, and maintaining plan of action
- mechanisms implementing continuous monitoring

### 3.12.2 *Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company information systems.*

Is there an action plan to remediate identified weaknesses or deficiencies?

Yes No Partially Does Not Apply Alternative Approach

Is the action plan maintained as remediation is performed?

Yes No Partially Does Not Apply Alternative Approach

Does the action plan designate remediation dates and milestones for each item?

Yes No Partially Does Not Apply Alternative Approach

Are deficiencies and weaknesses identified in security requirements assessments added to the action plan within a specified timeframe (e.g., 30 days) of the findings being reported?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional information**

Plans of Action should address how and when any unimplemented security requirements or partially met security requirements will be addressed, how any planned improvements will be implemented, and how and when deficiencies will be corrected and how they will reduce or eliminate vulnerabilities in the system. Companies can document the system security plan and plans of action as separate or combined documents in any chosen format

#### **Where to Look:**

- security assessment and authorization policy
- procedures addressing security assessment planning
- procedures addressing security assessments
- procedures addressing plan of action
- procedures addressing continuous monitoring of information system security requirements
- procedures addressing configuration management
- information system monitoring records
- configuration management records,
- security impact analyses
- status reports

- security assessment report
- security assessment evidence
- plan of action
- security assessment plan
- other relevant documents or records

#### **Who to Talk to:**

- employees with security assessment responsibilities
- employees with plan of action development and implementation responsibilities
- employees with continuous monitoring responsibilities
- employees with information security responsibilities
- system/network administrators

#### **Perform Test On:**

- automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting
- automated mechanisms for developing, implementing, and maintaining plan of action
- mechanisms implementing continuous monitoring

### 3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Are continuous monitoring tools deployed for front internet facing systems (computers with IP addresses that can be reached from the internet) or those used to store or transmit sensitive data?

Yes No Partially Does Not Apply Alternative Approach

At a minimum, are these systems monitored for privileged access, permission changes, kernel modifications, and binary changes against a control and system baseline?

Yes No Partially Does Not Apply Alternative Approach

Are continuous monitoring reports and alerts reviewed frequently (e.g., daily)?

Yes No Partially Does Not Apply Alternative Approach

Are unauthorized changes or unauthorized access reported to company management, and information system owner within a certain timeframe (e.g., 24 hours) of it being discovered?

Yes No Partially Does Not Apply Alternative Approach

Is there an assessor or assessment team to monitor the security requirement in the system on an ongoing basis?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Companies can maximize the value of assessments of security requirements during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process.

There is no defined period for security requirement assessments. The company should define for itself when requirements are assessed, which may be based on a timeframe determined by its needs and/ or events, such as a change to the system or its environment.

There is no prescribed format or level of specificity for a system security plan (see 3.12.4 System Security Plan), and DOD Contracting Officers/Requiring Activities should not prescribe a format or level of specificity. Per Chapter 3 of NIST SP 800-171, rev 1, "Organizations can document the

system security plan and plan of action as separate or combined documents and in any chosen format."

The complete system security plan can be quite sensitive and typically DOD does not need the description of system boundaries and operational environment (or other sensitive information that the company may have included in the system security plan to make it operationally useful for their purposes) to demonstrate the organization's implementation or planned implementation of the NIST SP 800-171 security requirements.

Accordingly, the requiring activity/contracting officer should not require in the solicitation that the actual system security plan be submitted, but rather an extract that describes how the individual security requirements are implemented, and any associated plans of action to implement security requirements not yet met. A company should tailor its submission, or extract of the system security plan, to provide only the information required by the solicitation, and avoid including sensitive information that is not required.

The requiring activity may specify in the solicitation, however, that the contractor must provide information in the technical proposal in a particular format and level of detail. This should NOT be interpreted as prescribing a particular format or level of detail for a contractor's system security plan or plans of action.

Also in accordance with Chapter 3 of NIST SP 800-171, rev 1, "federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization." As such, they may determine that the risk is such that they will not pursue an agreement or contract with the organization.

#### Where to Look:

- security assessment and authorization policy
- procedures addressing security assessment planning
- procedures addressing security assessments
- procedures addressing plan of action
- procedures addressing continuous monitoring of information system security requirements
- procedures addressing configuration management
- security plan
- security assessment plan

- security assessment report
- security assessment evidence
- plan of action
- information system monitoring records
- configuration management records,
- security impact analyses
- status reports
- other relevant documents or records

**Who to Talk to:**

- employees with security assessment responsibilities
- employees with plan of action development and implementation responsibilities
- employees with continuous monitoring responsibilities
- employees with information security responsibilities
- system/network administrators

**Perform Test On:**

- automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting
- automated mechanisms for developing, implementing, and maintaining plan of action
- mechanisms implementing continuous monitoring

**3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.**

Are system security plans consistent with the organization's enterprise architecture?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan explicitly define the authorization boundary for the system?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe the operational context of the system in terms of missions and business processes?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe the operational environment for the system?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe relationships with or connections to other systems?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan provide an overview of the security and privacy requirements for the system?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe the security requirements in place?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan include plans for meeting those requirements not yet in place?

Yes No Partially Does Not Apply Alternative Approach

Is the system security plan reviewed and approved by company management prior to plan implementation?

Yes No Partially Does Not Apply Alternative Approach

Are copies of the system security plan distribute to relevant company employees?

Yes No Partially Does Not Apply Alternative Approach

Are changes to the system security plan communicated to relevant company employees?

Yes No Partially Does Not Apply Alternative Approach

Does the company periodically review the system security plan within a certain timeframe? (e.g., annually)

Yes No Partially Does Not Apply Alternative Approach

Does the company update the system security plan to address changes to the system, environment of operation or problems identified during plan implementation or security assessments?

Yes No Partially Does Not Apply Alternative Approach

Does the company protect the system security plan from unauthorized disclosure and modification?

Yes No Partially Does Not Apply Alternative Approach

Does the company plan and coordinate security-related activities affecting the system before conducting any such activities?

Yes No Partially Does Not Apply Alternative Approach

Are security-related activities planned to reduce the impact on other company entities?

Yes No Partially Does Not Apply Alternative Approach

**Additional Information**

There is no prescribed format or specified level of detail for system security plans. However, companies must ensure that the required information in 3.12.4 is appropriately conveyed in those plans.

Some systems, including specialized systems (e.g., industrial/process control systems, Computer Numerical Control (CNC) machines), may have restrictions or limitations on the application of certain security requirements. To accommodate such issues, the system security plan should be used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies should be managed through plans of action.

System security plans describe how the company meets the security requirements but do not provide detailed, technical descriptions of the specific design or implementation. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to company operations and assets, employees, and other organizations, if the plan is implemented as intended.

System security plans need not be single documents. The plans can be a collection of various documents including documents that already exist within the company. Effective systems security plans make extensive use of references to policies, procedures,

and additional documents including, for example, design and implementation specifications where more detailed information can be obtained. This reduces the documentation associated with security programs and maintains the security-related information in other established management and operational areas including, for example, enterprise architecture, system development life cycle, systems engineering, and acquisition. System security plans do not contain detailed contingency plan or incident response plan information but instead provide sufficient information to define what needs to be accomplished by those plans.

**Where to Look:**

- security planning policy
- procedures addressing security plan development and implementation
- procedures addressing security plan reviews and updates
- enterprise architecture documentation
- security plan for the information system
- records of security plan reviews and updates
- other relevant documents or records

**Who to Talk to:**

- employees with security planning and plan implementation responsibilities
- employees with information security responsibilities

**Perform Test On:**

- automated mechanisms supporting system security plan development
- automated mechanisms for developing, implementing, and maintaining system security plans

### **Systems and Communications Protection: SP 800-171 Security Family 3.13**

System and communications protection requirements provide an array of safeguards for the system. Some of the requirements in this family address the confidentiality information at rest and in transit. The protection of confidentiality can be provided by these requirements through physical or logical means. For example, a company can provide physical protection by segregating certain functions to separate servers, each having its own set of IP addresses.

Companies can better safeguard their information by separating user functionality and system management functionality. Providing this type of protection prevents the presentation of system management-related functionality on an interface for non-privileged users. System and communications protection also establishes boundaries that restrict access to publicly accessible information within a system. Using boundary protections, a company can monitor and control communications at external boundaries as well as key internal boundaries within the system.

Examples of system and communication protection requirements include: application partitioning, denial of service protection, boundary protection, trusted path, mobile code, session authenticity, thin nodes, honeypots, transmission confidentiality and integrity, operations security, protection of information at rest and in transit, and usage restrictions. Companies should:

- monitor, control, and protect company communications (i.e., information transmitted or received by company 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 company systems.

The following security requirements fall under the Systems and Communication Protection family.



### 3.13.1 Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems.

Has the company identified network communications boundaries?

Yes No Partially Does Not Apply Alternative Approach

Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?

Yes No Partially Does Not Apply Alternative Approach

Do policies for managed interfaces such as gateways, routers, firewalls, VPNs, and company DMZs restrict external web traffic to only designated servers exist?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Portable media refers to storing and playing digital media such as audio, images and video files. The data is typically stored on a CD, DVD, flash memory, microdrive, or hard drive located on portable devices, and therefore can easily be taken outside of system boundaries.

Boundary protection refers to the monitoring and control of communications at the external boundary of an information system. Boundary protection is used to prevent and detect malicious and other unauthorized communications. Boundary protection devices may include gateways, routers, firewalls, guards, and encrypted tunnels.

#### Where to Look:

- system and communications protection policy
- procedures addressing boundary protection
- procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
- information security requirements and specifications
- list of key internal boundaries of the information system
- information system design documentation

- boundary protection hardware and software
- information system configuration settings and associated documentation
- enterprise security architecture documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with responsibility for determining information system security requirements
- employees with information system specification, design, development, implementation, and modification responsibilities
- information system developers
- employees with boundary protection responsibilities
- employees with information security responsibilities

#### Perform Test On:

- automated mechanisms implementing boundary protection capability
- automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

### 3.13.2 *Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within company information systems.*

Are the company's information security policies (including architectural design, software development, and system engineering principles) designed to promote information security?

Yes No Partially Does Not Apply Alternative Approach

Are the policies adequate to meet the needs of the company?

Yes No Partially Does Not Apply Alternative Approach

Are system security engineering principles applied in the specification, design, development, and implementation of the system?

Yes No Partially Does Not Apply Alternative Approach

Is the system managed using a system development life-cycle methodology that includes security considerations?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Companies should apply security engineering principles primarily to new development of information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include:

- developing layered protections
- establishing sound security policy
- architecture, and controls as the foundation for design
- incorporating security requirements into the system development life cycle
- delineating physical and logical security boundaries
- ensuring that system developers are trained on how to build secure software
- tailoring security requirements to meet company and operational needs
- performing threat modeling to identify use cases, threat agents, attack vectors, and

- attack patterns as well as compensating controls and design patterns needed to mitigate risk and reducing risk to acceptable levels, enabling informed risk management decisions

#### **Where to Look:**

- system and communications protection policy
- system and services acquisition policy procedures addressing boundary protection
- procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
- information security requirements and specifications for the information system
- list of key internal boundaries of the information system
- information system design documentation
- boundary protection hardware and software information
- system configuration settings and associated documentation
- enterprise security architecture documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- system developers
- employees with responsibility for determining information system security requirements
- employees with information system specification, design, development, implementation, and modification responsibilities
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms implementing boundary protection capability
- processes for applying security engineering principles in information system specification, design, development, implementation, and modification

- automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

### 3.13.3 *Separate user functionality from information system management functionality.*

Are physical or logical controls used to separate user functionality from system management-related functionality (e.g., to ensure that administration [e.g., privilege] options are not available to general users)?

Yes No Partially Does Not Apply Alternative Approach

Is user functionality separated from system management functionality?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Companies implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

#### **Where to Look:**

- system and communications protection policy
- procedures addressing application partitioning
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities

- system developers

#### **Perform Test On:**

- separation of user functionality from information system management functionality

### 3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

Are requirements implemented to prevent object reuse and to protect residual information?

Yes No Partially Does Not Apply Alternative Approach

Does the system prevent unauthorized or unintended information transfer via shared system resources, e.g., register, main memory, secondary storage?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

This requirement prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This requirement does not address information remanence which refers to residual representation of data that has been nominally erased or removed, covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions, or components within information systems for which there are only single users/roles.

#### Where to Look:

- system and communications protection policy
- procedures addressing information protection in shared system resources
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities

- system developers

#### Perform Test On:

- automated mechanisms preventing unauthorized and unintended transfer of information via shared system

### 3.13.5 *Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.*

Does the company implement DMZs?

Yes No Partially Does Not Apply Alternative Approach

Are they adequate to meet the needs of the company?

Yes No Partially Does Not Apply Alternative Approach

Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

In cybersecurity, a demilitarized zone (DMZ), sometimes referred to as a perimeter network, is a physical or logical subnetwork that contains and exposes a company's external-facing services to an untrusted network, usually a larger network such as the internet. The purpose of a DMZ is to add an additional layer of security to a company's LAN, an external network node can access only what is exposed in the DMZ, and can be intensely managed and audited, while the rest of the company's network is firewalled.

#### **Where to Look:**

- system and communications protection policy
- system and services acquisition policy
- procedures addressing boundary protection
- procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
- information system design documentation
- information security requirements and specifications
- list of key internal boundaries of the information system
- information system design documentation
- boundary protection hardware and software
- information system configuration settings and associated documentation
- enterprise security architecture

documentation

- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- system developer
- employees with boundary protection responsibilities
- employees with responsibility for determining information system security requirements
- employees with information system specification, design, development, implementation, and modification responsibilities
- information system developers
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms implementing boundary protection capability
- processes for applying security engineering principles in information system specification, design, development, implementation, and modification
- automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

### 3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Are all business need exceptions to network communications traffic (inbound/outbound) “deny all” policies documented?

Yes No Partially Does Not Apply Alternative Approach

Does the system deny network traffic by default and allow network traffic by exception?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Firewalls and routers placed at the perimeter of the system should only allowed traffic that is permitted to flow through. A permit by exception policy is used to allow the use of authorized programs.

#### **Where to Look:**

- system and communications protection

policy

- procedures addressing boundary protection
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- system developers
- employees with boundary protection responsibilities

#### **Perform Test On:**

- automated mechanisms implementing traffic management at managed interfaces

### 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.

Are controls in place to prevent split tunneling in remote devices, and to mandate VPN use when necessary for business functions?

Yes No Partially Does Not Apply Alternative Approach

Does the system prevent remote devices that have established connections (e.g., remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Split tunneling allows a mobile user to access dissimilar security domains like a public network (e.g., the internet) and a LAN or WAN at the same time, using the same or different network connections.

A VPN is a virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. A common example is a tunnel that connects an employee's laptop to the company's network.

#### Where to Look:

- system and communications protection policy
- procedures addressing boundary protection
- information system design documentation
- information system hardware and software
- information system architecture
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities

- system developer
- employees with boundary protection responsibilities

#### Perform Test On:

- automated mechanisms implementing boundary protection capability
- automated mechanisms supporting/restricting non-remote connections



### 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Are cryptographic mechanisms used to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures?

Yes No Partially Does Not Apply Alternative Approach

Are processes and automated mechanisms used to provide encryption of CUI during transmission?

Yes No Partially Does Not Apply Alternative Approach

Are all alternative physical safeguards used to provide confidentiality of CUI during transmission documented?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module must have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient. The module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

<http://csrc.nist.gov/groups/STM/cmvp/>

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor

information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS validated cryptography.

Encryption, though preferred, is not required if using common-carrier provided Multiprotocol Label Switching (MPLS) private network, as the MPLS separation provides sufficient protection without encryption.

Transport Layer Security (TLS) protocol can be used to protect CUI during transmission over the internet. The current version of TLS (TLS 1.2) is preferred. If earlier versions must be used to interact with certain organizations, the servers shall not support Secure Sockets Layer (SSL) version 3.0 or earlier. The cryptographic module used by the server and client must be a FIPS 140-validated cryptographic module. All cryptographic algorithms that are included in the configured cipher suites must be within the scope of the validation, as well as the random number generator. For further information see NIST SP 800-52, rev 1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations."

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>

#### Where to Look:

- system and communications protection policy
- procedures addressing transmission confidentiality and integrity
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security

responsibilities

- system developers

**Perform Test On:**

- automated mechanisms supporting and/or implementing transmission confidentiality and/ or integrity
- cryptographic mechanisms supporting and/or implementing transmission confidentiality and/ or integrity
- automated mechanisms supporting and/or implementing alternative physical safeguards
- processes for defining and implementing alternative physical safeguards

### 3.13.9 *Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.*

Does the system terminate a network connection at the end of a session or after a defined timeframe of inactivity?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This requirement applies to both internal and external networks. Time periods of inactivity may be established by companies and include time periods by type of network access or for specific network accesses.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

#### **Where to Look:**

- system and communications protection policy
- procedures addressing network disconnect
- information system design documentation
- security plan
- information system
- configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- system developers

#### **Perform Test On:**

- automated mechanisms supporting and/or implementing network disconnect capability

### 3.13.10 Establish and manage cryptographic keys for cryptography employed in the organization systems.

Are processes and automated mechanisms used to provide key management within the information system?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Cryptographic key management system provide for the management of cryptographic keys and their metadata including generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction.

#### Where to Look:

- system and communications protection policy
- procedures addressing cryptographic key establishment and management

- information system design documentation
- cryptographic mechanisms
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees with responsibilities for cryptographic key establishment and/or management

#### Perform Test On:

- automated mechanisms supporting and/or implementing cryptographic key establishment and management

### 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Is FIPS-validated cryptography used to protect CUI?

Yes No Partially Does Not Apply Alternative Approach

Do communication cryptographic mechanisms comply with applicable policies, standards, and guidance?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Cryptography can be employed to support a variety of security solutions including the protection of CUI, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography.

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module must have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient. The module (software and/ or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non- FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

<http://csrc.nist.gov/groups/STM/cmvp/>

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted

or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS-validated cryptography.

#### Where to Look:

- system and communications protection policy
- procedures addressing cryptographic protection
- information system design documentation
- information system configuration settings and associated documentation
- cryptographic module validation certificates
- list of FIPS validated cryptographic modules
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers
- employees with responsibilities for cryptographic protection

#### Perform Test On:

- automated mechanisms supporting and/or implementing cryptographic protection

### 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Have collaborative computing devices (e.g., cameras, microphones, etc.) been configured so they cannot be remotely activated?

Yes No Partially Does Not Apply Alternative Approach

Are users notified when collaborative computing devices are in use?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated.

#### Where to Look:

- system and communications protection policy
- procedures addressing collaborative computing
- access control policy and procedures
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers
- employees with responsibilities for managing collaborative computing devices

#### Perform Test On:

- automated mechanisms supporting and/or implementing management of remote activation of collaborative computing devices
- automated mechanisms providing an indication of use of collaborative computing devices

### 3.13.13 Control and monitor the use of mobile code.

Are there defined limits of mobile code usage, established usage restrictions, that specifically authorize use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript, etc.) within the information system?

Yes No Partially Does Not Apply Alternative Approach

Is the use of mobile code documented, monitored, and managed? (Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript, etc.)

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Decisions regarding the employment of mobile code within company information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within company information systems.

This requirement is necessary to protect the overall system processing CUI; it is not about software used to actually process CUI.

#### Where to Look:

- system and communications protection policy
- procedures addressing mobile code
- mobile code usage restrictions
- mobile code implementation policy and procedures
- list of acceptable mobile code and mobile code technologies
- list of unacceptable mobile code and mobile technologies
- authorization records
- information system monitoring records
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees with responsibilities for managing mobile code

#### Perform Test On:

- process for controlling, authorizing, monitoring, and restricting mobile code
- automated mechanisms supporting and/or implementing the management of mobile code
- automated mechanisms supporting and/or implementing the monitoring of mobile code

### 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Is the use of VoIP controlled?

Yes No Partially Does Not Apply Alternative Approach

Is the use of VoIP authorized, and monitored?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Voice Over Internet Protocol (VoIP) is a type of hardware and software that enables people to use the internet as the transmission pathway for telephone calls. VoIP sends voice data in packets by means of internet protocols (IP) instead of using traditional circuit transmissions of the public switched telephone network (PSTN).

Both the voice and data worlds come with the inherent IP security risks, when using the traditional voice side of the network through the application of VoIP. VoIP use necessitates security measures such as encrypting voice services, building redundancy into VoIP networks, locking down VoIP servers, and performing regular security audits on the network. It is also important that VoIP equipment is properly secured, it should be placed behind firewalls, and patched against vulnerabilities. VoIP should be monitored frequently using intrusion-detection systems.

If VoIP is physically or cryptographically isolated from the information systems processing CUI, this security requirement would not apply. However it is still prudent to control who uses VoIP since CUI could be taken from the information system and communicated via a VoIP system. Policies and procedures are needed to ensure CUI remains within the system that stores and processes it. See 3.1.2, 3.1.3, and 3.1.4 in the Access Control Family.

#### Where to Look:

- system and communications protection policy
- procedures addressing VoIP
- VoIP usage restrictions
- VoIP implementation guidance
- information system design documentation
- information system configuration settings and associated documentation
- information system monitoring records
- information system audit records

- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees with responsibilities for managing VoIP

#### Perform Test On:

- process for authorizing, monitoring, and controlling VoIP
- automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling VoIP



### 3.13.15 Protect the authenticity of communications sessions.

Are implemented controls in place to protect session communications (e.g., the controls implemented to validate identities and information transmitted to protect against man-in-the-middle attacks, session hijacking, and insertion of false information into sessions)?

Yes No Partially Does Not Apply Alternative Approach

Does the system provide mechanisms to protect the authenticity of device-to-device communications sessions?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This requirement addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services), and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

#### **Where to Look:**

- system and communications protection policy
- procedures addressing session authenticity
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities

#### **Perform Test On:**

- automated mechanisms supporting and/or implementing session authenticity

### 3.13.16 Protect the confidentiality of CUI at rest.

Are there controls used to protect CUI while stored in company information systems?

Yes No Partially Does Not Apply Alternative Approach

Does the system protect the confidentiality of information at rest?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

This requirement addresses the confidentiality of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Companies may also employ other security requirements including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

CUI can be stored at rest in any non-mobile devices or data center, unencrypted, as long as it is protected by other approved logical or physical methods. The mapped NIST SP 800-53, “Security Controls and Assessment Procedures for Federal Information Systems and Organizations,” control (SC-8), notes that this requirement is to protect the confidentiality of CUI information at rest when it is located on storage devices as specific components of information systems and that “organizations may employ different mechanisms to achieve confidentiality protection, including the use of cryptographic mechanisms and file share scanning.” Thus, encryption is an option, not a requirement.

#### **Where to Look:**

- system and communications protection policy
- procedures addressing protection of information at rest
- information system design documentation
- information system configuration settings and associated documentation
- cryptographic mechanisms and associated configuration documentation

- list of information at rest requiring confidentiality and integrity protections
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- system developers

#### **Perform Test On:**

- automated mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest

### **System and Information Integrity: SP 800-171 Security Family 3.14**

Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. It is the assertion that data can only be accessed or modified by the authorized employees. System and information integrity provides assurance that the information being accessed has not been meddled with or damaged by an error in the system. Examples of system and information integrity requirements include: flaw remediation, malicious code protection, security function verification, information input validation, error handling, non-persistence, and memory protection.

Companies should

- identify, report, and correct information and system flaws in a timely manner,
- provide protection from malicious code at appropriate locations within company systems, and
- monitor system security alerts and advisories and respond appropriately.

The following security requirements fall under the System and Information Integrity family.

### 3.14.1 Identify, report, and correct information and information system flaws in a timely manner.

Are system flaws identified, reported, and corrected within company-defined time periods?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform all security-relevant software updates (patching, service packs, hot fixes, and anti-virus signature additions) in response to identified system flaws and vulnerabilities within the timeframe specified in policy or within the system security plan?

Yes No Partially Does Not Apply Alternative Approach

When available, do managers and administrators of the system rely on centralized management of the flaw remediation process, to include the use of automated update software, patch management tools, and automated status scanning?

Yes No Partially Does Not Apply Alternative Approach

Is the time between flaw identification and flaw remediation measured and compared with benchmarks?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Companies identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to employees with information security responsibilities. Security-relevant software updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in company information systems.

By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the

criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Companies determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, companies may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Companies may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

#### Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code
- procedures addressing security alerts, advisories, and directives
- records of security alerts and advisories
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)

- test results from the installation of software and firmware updates to correct information system flaws
- installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

**Who to Talk to:**

- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with configuration management responsibility
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, company elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
- system/network administrators
- employees with information security responsibilities

**Perform Test On:**

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates
- automated mechanisms supporting and/or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing testing software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms

- process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

### 3.14.2 *Provide protection from malicious code at appropriate locations within organization information systems.*

Does the company employ malicious code protection mechanisms at system entry and exit points to minimize the presence of malicious code? System entry and exit points may include firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices.

Yes No Partially Does Not Apply Alternative Approach

Does the system automatically update malicious code protection mechanisms?

Yes No Partially Does Not Apply Alternative Approach

#### **Additional Information**

Malicious code protection mechanisms (e.g., anti-virus, anti-malware and anti-spyware) include, for example, signature definitions, heuristics, and behavior analyzers. Due to information system integrity and availability concerns, companies should consider the methodology used to carry out automatic updates.

#### **Where to Look:**

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code protection
- procedures addressing security alerts, advisories, and directives
- records of security alerts and advisories  
other relevant documents or records
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection

mechanisms

- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- test results from the installation of software and firmware updates to correct information system flaws installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

#### **Who to Talk to:**

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
- employees with configuration management responsibility

#### **Perform Test On:**

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates

- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing testing software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

### 3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.

Does the company receive security alerts, advisories, and directives from reputable external organizations?

Yes No Partially Does Not Apply Alternative Approach

Does the company disseminate this information to individuals with need-to-know in the company?

Yes No Partially Does Not Apply Alternative Approach

Are alerts responded to in a timely manner?

Yes No Partially Does Not Apply Alternative Approach

Are internal security alerts, advisories, and directives generated?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness: <https://www.us-cert.gov/>

Security directives are issued by designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on company operations and assets, individuals, and other organizations, should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

Cleared defense contractors are eligible for the Defense Industrial Base (DIB) Cybersecurity program, which is a voluntary cyber threat information sharing program between DOD and DIB participants. Under this partnership, the DOD Cyber Crime Center receives voluntary reporting from DIB participants and makes available to all the other DIB participants, as well as indicators from Government sources. See <https://dibnet.dod.mil/portal/intranet/>

#### Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation

- procedures addressing malicious code protection
- procedures addressing security alerts, advisories, and directives records of security alerts and advisories
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- testing results from the installation of software and firmware updates to correct information system flaws
- installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

#### Who to Talk to:

- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with configuration management responsibility
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, company elements, and/or external



organizations to whom alerts, advisories, and directives are to be disseminated

- system/network administrators
- employees with information security responsibilities

**Perform Test On:**

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates
- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing test software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

### 3.14.4 Update malicious code protection mechanisms when new releases are available.

Does the company update information system protection mechanisms (e.g., anti-virus signatures) within 5 days of new releases?

Yes No Partially Does Not Apply Alternative Approach

Are these updates completed in accordance with configuration management policy and procedures?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect company business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, companies should rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than those intended. Companies may determine that in response to the detection of malicious code, different actions may be warranted. For example, companies can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

#### Where to Look:

- system and information integrity policy

- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code protection
- procedures addressing security alerts, advisories, and directives
- records of security alerts and advisories other relevant documents or records
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- test results from the installation of software and firmware updates to correct information system flaws installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system

- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
- employees with configuration management responsibility

**Perform Test On:**

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates
- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing testing software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

### 3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Does the company perform periodic scans of the information system for malware? Are scans performed within the timeframe specified in policy or within the system security plan?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform real-time scans of files from external sources as the files are downloaded, opened, or executed?

Yes No Partially Does Not Apply Alternative Approach

Does the system disinfect and quarantine infected files?

Yes No Partially Does Not Apply Alternative Approach

#### Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing malicious code protection
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for malicious

code protection

- employees with configuration management responsibility

#### Perform Test On:

- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions

### 3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Does the company monitor the information system to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections?

Yes No Partially Does Not Apply Alternative Approach

Will the company strategically deploy monitoring devices within the information system to collect essential information?

Yes No Partially Does Not Apply Alternative Approach

Is the information gained from these monitoring tools protected from unauthorized access, modification, and deletion?

Yes No Partially Does Not Apply Alternative Approach

Does the system monitor inbound and outbound communications for unusual or unauthorized activities or conditions?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code within company information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems.

Evidence of malicious code is used to identify potentially compromised information systems or information system components. Monitoring of these communications may indicate or detect potential attacks to the company's information system.

#### Where to Look:

- continuous monitoring strategy
- system and information integrity policy
- procedures addressing information system monitoring tools and techniques
- facility diagram/layout information
- system design documentation
- information system monitoring tools and techniques

- documentation locations within information system where monitoring devices are deployed
- information system configuration settings and associated documentation
- information system protocols
- information system audit records
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility monitoring the information system
- employees with responsibility for the intrusion detection system

#### Perform Test On:

- processes for information system monitoring
- automated mechanisms supporting and/or implementing information system monitoring capability
- processes for intrusion detection/information system monitoring
- automated mechanisms supporting and/or implementing intrusion detection capability/information system monitoring
- automated mechanisms supporting and/or implementing monitoring of inbound/ outbound communications traffic

### 3.14.7 Identify unauthorized use of the information system.

Does the company monitor the information system to identify unauthorized access and use?

Yes No Partially Does Not Apply Alternative Approach

Does the company monitor the information for potential misuse?

Yes No Partially Does Not Apply Alternative Approach

Is unauthorized use of the system identified (e.g., log monitoring)?

Yes No Partially Does Not Apply Alternative Approach

#### Additional Information

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system.

Companies can monitor information systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces.

The granularity of monitoring information collected is based on company monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, hyper text transfer protocol (HTTP) traffic that bypasses HTTP proxies.

Information system monitoring is an integral part of company continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, internet). A remote connection is any connection with a device communicating through an external network (e.g., the

internet). Local, network, and remote connections can be either wired or wireless.

#### Where to Look:

- continuous monitoring strategy
- system and information integrity policy
- procedures addressing information system monitoring tools and techniques
- facility diagram/layout information
- system design documentation
- information system monitoring tools and techniques
- documentation locations within information system where monitoring devices are deployed
- information system configuration settings and associated documentation
- other relevant documents or records

#### Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility monitoring the information system

#### Perform Test On:

- processes for information system monitoring
- automated mechanisms supporting and/or implementing information system monitoring capability

## Glossary

**Access Control** - The process of granting or denying specific requests to: 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

**Accountability** - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

**Adware** - Advertising-supported software is any software package that automatically renders advertisements to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. Unwanted advertisements are considered malware.

**Assurance** - Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes 1) functionality that performs correctly, 2) sufficient protection against unintentional errors (by users or software), and 3) sufficient resistance to intentional penetration or by-pass.

**Attack** - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

**Audit** - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

**Audit log** - Chronological record of system activities, including records of system accesses and operations performed in a given period.

**Audit record** - Individual entry in an audit log related to an audited event.

**Authentication** - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

**Authorization** - The official management decision given by a senior official to authorize operation of a system or the common controls inherited by designated organizations systems and to explicitly accept the risk to company operations (including mission, functions, image, and reputation), company assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Also known as authorization to operate (ATO).

**Authorizing Official (AO)** - A senior (federal) official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to company operations (including mission, functions, image, or reputation), company assets, individuals, other organizations, and the Nation.

**Availability** - Ensuring timely and reliable access to and use of information.

**Back Door** - An undocumented way of gaining access to computer system. A backdoor is a potential security risk.

**Baseline Configuration** - A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

**Blacklisting** - A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.

**Biometrics** - A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

**Bit** - A binary digit having a value of 0 or 1.

**Challenge Response Protocol** - An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.

**Checksum** - A value that 1) is computed by a function that is dependent on the content of a data object and 2) is stored or transmitted together with the object, for detecting changes in the data.

**Ciphertext** - Data in its encrypted form.

**Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Configuration Management** - A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

**Configuration Settings** - The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.

**Controlled Area** - Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

**Controlled Unclassified Information (CUI)** - Information that law, regulation, or government wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

**CUI Categories or Subcategories** - Those types of information for which laws, regulations, or government wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.

**CUI Executive Agent** - The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to



comply with Executive Order 13556 “Controlled Unclassified Information”. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

**CUI Program** - The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.

**CUI Registry** - The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

**Countermeasures** - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

**Denial of Service** - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

**Decoding** - The conversion of an encoded format back into the original sequence of characters.

**Digital Signature** - The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1) origin authentication, 2) data integrity, and 3) signer non-repudiation.

**Encoding** - To convert into a coded form; the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage.

**Encryption** - The cryptographic transformation of data to produce ciphertext.

**End-to-End Encryption** - Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.

**Environment of Operation** - The physical surroundings in which a system processes, stores, and transmits information.

**Executive Agency** - An executive department specified in 5 U.S.C., Sec. 105; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

**External System (or component)** - A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

**External System Service** - A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

**External System Service Provider** - A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

**External Network** - A network not controlled by the organization.

**Federal Information System** - An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

**FIPS-validated cryptography** - A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP).

**Firewall** - A gateway that limits access between networks in accordance with local security policy.

**Firmware** - Computer programs and data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the programs and data cannot be dynamically written or modified during execution of the programs.

**Gateway** - An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.

**Hacker** - A person who circumvents security and breaks into a network, computer, file, etc., usually with malicious intent.

**Hardware** - The physical components of a system.

**Identifier** - Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.

**Impact** - The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.

**Impact Value** - The assessed potential impact resulting from a compromise of the confidentiality of information (e.g., CUI) expressed as a value of low, moderate, or high.

**Incident** - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**Industrial Control System (ICS)** – A general term that encompasses several types of control systems and associated instrumentation used in industrial production technology, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS),

and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

Information - 1) Facts and ideas, which can be represented (encoded) as various forms of data. 2) Knowledge, e.g., data, instructions, in any medium or form that can be communicated between system entities.

Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Flow Control - Procedure to ensure that information transfers within a system are not made in violation of the security policy.

Information Resources - Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information Security Policy - Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information Security Risk - The risk to company operations (including mission, functions, image, reputation), company assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or a system.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information Technology - (A) With respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use - 1) of that equipment or 2) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

Insider Threat - The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the

United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Internal Network** - A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization controlled endpoints, provides the same effect (with regard

to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization- controlled while not being organization-owned.

**Intrusion Detection System (IDS)** - Software that automates the intrusion detection process.

**Key** - A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include: 1) the computation of a digital signature from data, and 2) the verification of a digital signature.

**Key Management** - The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use, and destruction.

**Keystroke Monitoring** - The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

**Least Privilege** - The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

**Link Encryption** - Encryption of information between nodes of a communications system.

**Local Access** - Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

**Logic Bomb** - A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

**Malicious Code** - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

**Malware** - See Malicious Code.

**Media** - Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.

**Mobile Code** - Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

**Mobile Device** - A portable computing device that has a small-form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.

**Multifactor Authentication** - Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).

**Network** - A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

**Network Access** - Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, internet).

**Node** - In data communication, a physical network node may either be a data communication equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment (DTE) such as a digital telephone handset, a printer or a computer, workstation, or a server.

**Nonce** - A time-varying value that has at most a negligible chance of repeating – for example, a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these.

**Nonfederal Organization** - An entity that owns, operates, or maintains a nonfederal information system.

**Nonfederal System** - A system that does not meet the criteria for a federal system.

**Nonlocal Maintenance** - Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

**Password** - A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

**Penetration Performance Testing** - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

**Phishing** - A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

**Portable Storage Device** - A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/ thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).

**Potential Impact** - The loss of confidentiality, integrity, or availability could be expected to have: 1) a limited adverse effect (FIPS Publication 199 low); 2) a serious adverse effect (FIPS

Publication 199 moderate); or 3) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

**Private Key** - A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

**Privilege** - A right granted to an individual, a program, or a process.

**Privileged Account** - A system account with authorizations of a privileged user.

**Privileged User** - A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

**Public Key** - A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.

**Public Key Cryptography** - Encryption system that uses a public-private key pair for encryption and/or digital signature.

**Public Key Infrastructure (PKI)** - A Framework that is established to issue, maintain, and revoke public key certificates.

**Ransomware** - Ransomware is a type of malware that blocks access to a device or data until a ransom is paid.

**Reciprocity** - Mutual agreement among participating enterprises to accept each other's security assessments to reuse information system resources and/or to accept each other's assessed security posture to share information.

**Records** - The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the system are performing as intended. Also, used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

**Remote Access** - Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the internet).

**Remote Maintenance** - Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).

**Replay Resistance** - Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

**Risk** - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: 1) the adverse impacts that would arise if the circumstance or event occurs and 2) the likelihood of occurrence. Note: System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems and reflect the potential adverse impacts to company operations (including mission, functions, image, or reputation), company assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to systems that support critical

infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

**Risk Assessment** - The process of identifying risks to company operations (including mission, functions, image, and reputation), company assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with Risk Analysis.

**Risk Management** - The program and supporting processes to manage information security risk to company operations (including mission, functions, image, reputation), company assets, individuals, other organizations, and the Nation, and includes: 1) establishing the context for risk-related activities, 2) assessing risk, 3) responding to risk once determined, and 4) monitoring risk over time.

**Risk Management Framework (RMF)** - A structured approach used to oversee and manage risk for an enterprise.

**Role** - A job function or employment position to which people or other system entities may be assigned in a system.

**Safeguards** - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

**Sanitization** - Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

**Secret Key** - A cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public.

**Security** - A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

**Security Control Assessment** - The testing and/or evaluation of the management, operational, and technical security controls in a system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

**Security Controls** - The management, operational, and technical controls, i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information.

**Security Engineering** - An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and

required functionality early in the systems development life cycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

**Security Functionality** - The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational systems or the environments in which those systems operate.

**Security Functions** - The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

**Security Label** - The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.

**Security Relevance** - Functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.

**Sensitivity** - A measure of the importance assigned to information by its owner for the purpose of denoting its need for protection.

**Signature** - A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

**SMiShing (SMS phishing)** - A security attack in which the user is tricked into downloading a Trojan horse, virus, or other malware onto his cellular phone or other mobile device.

**Spam** - Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

**Split Tunneling** - The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.

**Spyware** - Software that is secretly or surreptitiously installed into a system to gather information on individuals or organizations without their knowledge; a type of malicious code.

**Supplemental Guidance** - Statements used to provide additional explanatory information for security controls or security control enhancements.

**System** - Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

**System Component** - A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.

**System Integrity** - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.



**System Security Plan** - Formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.

**Tailoring** - The process by which a security control baseline is modified based on: 1) the application of scoping guidance, 2) the specification of compensating security controls, if needed, and 3) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

**Threat** - Any circumstance or event with the potential to adversely impact company operations (including mission, functions, image, or reputation), company assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Threat Event** - An event or situation that has the potential for causing undesirable consequences or impact.

**Token** - Something that the claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.

**Trojan Horse** - A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

**Trusted Computing Base** - Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

**Trustworthy System Computer** - Hardware, software and procedures that - 1) are reasonably secure from intrusion and misuse, 2) provide a reasonable level of availability, reliability, and correct operation, and 3) are reasonably suited to performing their intended functions and 4) adhere to generally accepted security procedures.

**User** - Individual, or a process acting on behalf of an individual, authorized to access a system.

**Validation** - Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes.)

**Virus** - A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See Malicious Code.

**Vishing** - The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

**Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Whitelisting - A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.

Wireless Technology - Technology that permits the transfer of information between separated points without physical connection.

Worm - A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code.

## **Appendix A: Useful Plans, Policies and Procedures**

**Plans you should have in place:**

- Business Continuity Plans
- Contingency Plans
- Continuity of Operations Plans
- Critical Infrastructure Plans
- Crisis Communications Plan
- Disaster Recovery Plans
- Incident Response Plan
- Incident Response Testing Plan
- Occupant Emergency Plan
- Physical/Environmental Protection Plan
- Plan of Action
- Security Assessment Plan
- Security Plan
- System Security Plan

**Policies and Procedures you should have:**

- Access Control
- Audit and Accountability
- Configuration Management
- Configuration Planning
- Incident Response

- Identification and Authentication
- Information Flow Control
- Information Flow Enforcement
- Information System Maintenance
- Media Protection
- Media Sanitization and Disposal
- Mobile Code Implementation
- Password
- Personnel Security
- Physical and Environmental Protection
- Portable Media
- Risk Assessment
- Security Assessment and Authorization
- Security Awareness and Training
- Security Planning
- Separation of Duties
- System and Information Integrity
- System and Services Acquisition
- System and Communication Protection
- System Use



# Cyber Incident Reporting

## *A Unified Message for Reporting to the Federal Government*

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

### **When to Report to the Federal Government**

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

### **What to Report**

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

### **How to Report Cyber Incidents to the Federal Government**

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

### **Types of Federal Incident Response**

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact	
Threat Response	Asset Response
<p><b>Federal Bureau of Investigation (FBI)</b></p> <p><b>FBI Field Office Cyber Task Forces:</b>  <a href="http://www.fbi.gov/contact-us/field">http://www.fbi.gov/contact-us/field</a></p> <p><b>Internet Crime Complaint Center (IC3):</b>  <a href="http://www.ic3.gov">http://www.ic3.gov</a></p> <p><i>Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.</i></p> <p><i>Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.</i></p>	<p><b>National Cybersecurity and Communications Integration Center (NCCIC)</b></p> <p><b>NCCIC:</b> (888) 282-0870 or <a href="mailto:NCCIC@hq.dhs.gov">NCCIC@hq.dhs.gov</a></p> <p><b>United States Computer Emergency Readiness Team:</b>  <a href="http://www.us-cert.gov">http://www.us-cert.gov</a></p> <p><i>Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.</i></p>
<p><b>National Cyber Investigative Joint Task Force</b></p> <p><b>NCIJTF CyWatch 24/7 Command Center:</b> (855) 292-3937 or <a href="mailto:cywatch@ic.fbi.gov">cywatch@ic.fbi.gov</a></p> <p><i>Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.</i></p>	
<p><b>United States Secret Service</b></p> <p><b>Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):</b>  <a href="http://www.secretservice.gov/contact/field-offices">http://www.secretservice.gov/contact/field-offices</a></p> <p><i>Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information</i></p>	
<p><b>United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)</b></p> <p><b>HSI Tip Line:</b> 866-DHS-2-ICE (866-347-2423) or <a href="https://www.ice.gov/webform/hsi-tip-form">https://www.ice.gov/webform/hsi-tip-form</a></p> <p><b>HSI Field Offices:</b> <a href="https://www.ice.gov/contact/hsi">https://www.ice.gov/contact/hsi</a></p> <p><b>HSI Cyber Crimes Center:</b> <a href="https://www.ice.gov/cyber-crimes">https://www.ice.gov/cyber-crimes</a></p> <p><i>Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.</i></p>	
<p><b>If there is an immediate threat to public health or safety, the public should always call 911.</b></p>	

# *NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1*

## **Table of Contents**

- 1) Background
- 2) Purpose
- 3) Strategically Assessing a Contractor's Implementation of NIST SP 800-171
- 4) Levels of Assessment
- 5) *NIST SP 800-171 DoD Assessment Scoring Methodology*
- 6) Documenting *NIST SP 800-171 DoD Assessment Results*
- 7) Glossary of Terms

Annex A - *NIST SP 800-171 DoD Assessment Scoring Template*

Annex B - Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment Results Format*



## 1) Background

- a) Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors and subcontractors to provide ‘adequate security’ to safeguard covered defense information, hereto referred to, for the purposes of this methodology, as Department of Defense (DoD) controlled unclassified information (CUI)<sup>1</sup>, when residing on or transiting through a contractor’s/subcontractor’s internal information system or network, and to report cyber incidents that affect that system or network to DoD. DFARS clause 252.204-7012 further states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. Contractors are also required to flow down DFARS Clause 252.204-7012 to all subcontracts for operationally critical support, or for which subcontract performance will involve DoD CUI. Contractors must mark or otherwise identify, in accordance with direction contained within the specific contract, DoD CUI that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract.
- b) DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires, among other things, offerors to represent they will implement the security requirements in NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the contracting officer. To document implementation of NIST SP 800-171, the contractor must develop, document, and periodically update a system security plan that describes system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. If implementation of the security requirements is not complete, companies must develop and implement plans of action to describe when and how any unimplemented security requirements will be met.
- c) Under Secretary of Defense (Acquisition and Sustainment) (USD(A&S)) memorandum, “Strategically Implementing Cybersecurity Contract Clauses,” dated February 5, 2019, directed the Defense Contract Management Agency (DCMA) to pursue, with companies for which they administer contracts, the application of a standard methodology and approach to assess a contractor’s implementation of NIST SP 800-171 at a strategic (corporate-wide) level as an alternative to the requirement for

---

<sup>1</sup> DoD is transitioning from the use of the term ‘covered defense information’ in the DFARS to “DOD Controlled Unclassified Information (CUI), [consistent with DoDI 5200.48, Controlled Unclassified Information \(CUI\)](#)”

contractors to document implementation of NIST SP 800-171 on a contract-by-contract basis.

## 2) Purpose

- a) The *NIST SP 800-171 DoD Assessment Methodology, Version 1.2* documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012.
- b) This methodology is used for assessment purposes only and does not, and is not intended to, add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012.
- c) DoD will use this methodology to assess the implementation of NIST SP 800-171 by its prime contractors. Prime contractors may use this methodology to assess the implementation status of NIST SP 800-171 by subcontractors.
- d) This methodology informed the conduct of pilot *NIST SP 800-171 DoD Assessments* performed by DCMA, in partnership with the Defense Counterintelligence and Security Agency (DCSA) and the DoD Components, during 2019. DoD will update and codify this methodology in policy/regulation.

## 3) Strategically Assessing a Contractor's Implementation of NIST SP 800-171

- a) The *NIST SP 800-171 DoD Assessment Methodology* enables DoD to strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts which include DFARS clause 252.204-7012, and to provide DoD Components with visibility to the summary level scores of strategic assessments completed by DoD, thus providing an alternative to the contract-by-contract approach.
- b) The *NIST SP 800-171 DoD Assessment* consists of three levels of assessments (see Section 4 of this document). These three types of assessments reflect the depth of the assessment, and the associated level of confidence in the assessment results.
- c) Assessment of contractors with contracts containing DFARS clause 252.204-7012 is anticipated to be once every three years unless other factors, such as program criticality/risk or a security-relevant change, drive the need for a different assessment frequency.

## 4) Levels of Assessment

- a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*
  - i) The Basic Assessment is the Contractor's self-assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information” and Section 5 and Annex A of this document.

- ii) The Basic Assessment results in a confidence level of ‘Low’ in the resulting score because it is a self-generated score.
  - iii) The summary level scores resulting from Basic *NIST SP 800-171 DoD Assessments* should be documented as indicated in Section 6 and Annex B of this document.
- b) Medium *NIST SP 800-171 DoD Assessment*
- i) The Medium Assessment is conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment. It is anticipated that Medium Assessments will be conducted primarily by Program Management Office cybersecurity personnel, as part of a separately scheduled visit (e.g., for a Critical Design Review).
  - ii) The assessment will consist of a review of the system security plan description of how each requirement is met to identify any descriptions which may not properly address the security requirements.
  - iii) The Medium Assessment results in a confidence level of ‘Medium’ in the resulting score.
  - iv) The DoD assessor will document summary level scores resulting from Medium *NIST SP 800-171 DoD Assessments* as indicated in Section 6 of this document.
- c) High (On-Site *or Virtual*) *NIST SP 800-171 DoD Assessment*
- i) The High Assessment, conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment, requires a thorough on-site *or virtual*<sup>2</sup> verification/examination/demonstration of the Contractor’s system security plan and implementation of the NIST SP 800-171 security requirements.
  - ii) *The High Assessment* is conducted using NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information.” The assessment will determine if the implementation meets the requirements by reviewing appropriate evidence and/or demonstration (e.g., recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication).
  - iii) *An on-site High NIST SP 800-171 DoD Assessment is the preferred methodology for a full evaluation of the risk to DoD CUI because of the ability to verify and validate the effectiveness of the safeguards that implement security*

---

<sup>2</sup> A virtual High Assessment was developed in response to the COVID-19 epidemic to allow protections of assessors and DIB personal to limit travel and exposure of staffs whilst still being able to assess contractor risk. The government may utilize this methodology in the future as required in response to similar or other scenarios.

requirements defined in NIST Special Publication 800-171. While a High Assessment maybe be conducted virtually in lieu of onsite, a virtual assessment will not fully cover all the NIST SP 800-171 requirements, resulting in a less than full understanding of overall risk.

- iv) A virtual High Assessment utilizes the same methodology as the on-site with added data protections processes enacted to protect the DIB data that is shared with assessment teams. All data is transmitted through DoD Secure Access File Exchange (SAFE), is only reviewed locally on each assessor's computer (screen sharing is conducted utilizing DoD collaboration mediums that are approved for processing CUI) and contractor data is destroyed post assessment using NSA guidance for data destruction. With concurrence from the DIB companies being assessed, the assessment verifies and examines all documents utilizing the NIST SP 800-171A methodology minus the demonstration or testing of some requirements. In some cases, a follow-up on-site assessment of the items not assessed may be required or requested.
  - v) The first step in a High Assessment is for the contractor to conduct a Basic Assessment and submit results to the Department using the procedures in Annex B of this document. The High Assessment consists of a review of the Basic Assessment, a thorough document review and discussion with the contractor regarding the results to obtain additional information or clarification as needed, combined with government validation that the security requirements have been implemented as described in the system security plan. Network access by the assessor(s) is not required.
  - vi) The High Assessment results in a confidence level of 'High' in the resulting score.
  - vii) The DoD assessor will document summary level scores resulting from High *NIST SP 800-171 DoD Assessments* as indicated in Section 6 of this document.
- 5) *NIST SP 800-171 DoD Assessment* Scoring Methodology
- a) This scoring methodology is designed to provide an objective assessment of a contractor's NIST SP 800-171 implementation status. With the exception of requirements for which the scoring of partial implementation is built-in (e.g., multi-factor authentication, security requirement 3.5.3) the methodology is not designed to credit partial implementation.
  - b) Conduct of the *NIST SP 800-171 DoD Assessment* will result in a score reflecting the net effect of security requirements not yet implemented. If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements. For each security requirement not met, the associated value is subtracted from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.

- c) While NIST SP 800-171 does not prioritize security requirements, certain requirements have more impact on the security of the network and its data than others. This scoring methodology incorporates this concept by weighting each security requirement based on the impact to the information system and the DoD CUI created on or transiting through that system, when that requirement is not implemented.
- d) Weighted requirements include all of the fundamental NIST SP 800-171 'Basic Security Requirements' - high-level requirements which, if not implemented, render ineffective the more numerous 'Derived Security Requirements'; and a subset of the 'Derived Security Requirements' - requirements that supplement the Basic Security Requirements - which, if not implemented, would allow for exploitation of the network and its information.
  - i) For security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of DoD CUI, 5 points are subtracted from the score of 110. For example, failure to limit system access to authorized users (Basic Security Requirement 3.1.1) renders all the other Access Control requirements ineffective, allowing easy exploitation of the network; failure to control the use of removable media on system components (Derived Security Requirement 3.8.7) could result in massive exfiltration of CUI and introduction of malware.
    - (1) Basic Security Requirements with a value of 5 points include 3.1.1, 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.1, 3.4.2, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.7.2, 3.8.3, 3.9.2, 3.10.1, 3.10.2, 3.12.1, 3.12.3, 3.13.1, 3.13.2, 3.14.1, 3.14.2, and 3.14.3.
    - (2) Derived Security Requirements with a value of 5 points include 3.1.12, 3.1.13, 3.1.16, 3.1.17, 3.1.18, 3.3.5, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.5.10, 3.7.5, 3.8.7, 3.11.2, 3.13.5, 3.13.6, 3.13.15, 3.14.4, and 3.14.6.
  - ii) For Basic and Derived Security Requirements that, if not implemented, have a specific and confined effect on the security of the network and its data, 3 points are subtracted from the score of 110. For example, failure to limit access to CUI on system media to authorized users (Security Requirement 3.8.2) or failure to encrypt CUI stored on a mobile device (Security Requirement 3.1.19), put the CUI stored on the system media or mobile device at risk, but not the CUI stored on the network itself.
    - (1) Basic Security Requirements with a value of 3 points include 3.3.2, 3.7.1, 3.8.1, 3.8.2, 3.9.1, 3.11.1, and 3.12.2.
    - (2) Derived Security Requirements with a value of 3 points include 3.1.5, 3.1.19, 3.7.4, 3.8.8, 3.13.8, 3.14.5, and 3.14.7.
  - iii) All remaining Derived Security Requirements, if not implemented, have a limited or indirect effect on the security of the network and its data. For these, 1 point

is subtracted from the score of 110. For example, failing to prevent reuse of identifiers for a defined period (Security Requirement 3.5.5) could allow a user access to CUI to which they were not approved.

- e) Two Derived Security Requirements can be partially effective even if not completely or properly implemented, and the points deducted should be adjusted depending on how the security requirement is implemented.
  - i) Multi-factor authentication (MFA) (Security Requirement 3.5.3) is typically implemented first for remote and privileged users (since these users are both limited in number and more critical) and then for the general user, so 3 points are subtracted from the score of 110 if MFA is implemented only for remote and privileged users; 5 points are subtracted from the score of 110 if MFA is not implemented for any users.
  - ii) FIPS validated encryption (Security Requirement 3.13.11) is required to protect the confidentiality of CUI. If encryption is employed, but is not FIPS validated, 3 points are subtracted from the score of 110; if encryption is not employed, 5 points are subtracted from the score of 110.
- f) Although not common, future revisions of NIST SP 800-171 may add, delete or substantively revise security requirements. When this occurs, a value will be assigned to any new or modified requirements in accordance with this scoring methodology.
- g) The contractor must have a system security plan (Basic Security Requirement 3.12.4) in place to describe each covered contractor information system, and a plan of action (Basic Security Requirement 3.12.2) in place for each unimplemented security requirement to describe how and when the security requirement will be met.
  - i) Since the NIST SP 800-171 DoD Assessment scoring methodology is based on the review of a system security plan describing how the security requirements are met, it is not possible to conduct the assessment if the information is not available. The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'
  - ii) Plans of action addressing unimplemented security requirements are not a substitute for a completed requirement. Security requirements not implemented, whether a plan of action is in place or not, will be assessed as 'not implemented.' For example, if the initial roll-out of 3.5.3, multifactor authentication, is only 75% complete, and there is a plan of action still being implemented, 3.5.3 will be considered 'not implemented', as the requirement has not been fully implemented.
  - iii) A lack of plan of action for unimplemented security requirements will result in Security Requirement 3.12.2 being assessed as 'not implemented.'

- h) Temporary deficiencies and/or isolated enduring exceptions which occur during initial implementation, or arise after implementation, are to be expected in most complex environments.
  - i) Temporary deficiencies that are appropriately addressed in plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) should be assessed as 'implemented.' For example, when a plan of action addresses a 'temporary deficiency' that arises after implementation (e.g., 3.13.11, employ FIPS validated cryptography, had been implemented, but subsequently a patch invalidated the FIPS validation of a particular cryptographic module), the requirement will be scored 'as implemented.' A 'temporary deficiency' may also arise during initial implementation of a NIST SP 800-171 requirement if, during roll-out, specific issues with certain equipment is discovered that has to be separately addressed (e.g., certain specific hardware or software unexpectedly needs to be changed for the requirement to be successfully applied). If the implementation roll-out has otherwise been completed, this 'temporary deficiency' plan of action would be considered, and the requirement scored 'as implemented.' There is no standard duration for which a 'temporary deficiency' may be active. It is what is reasonable, which would take into consideration the availability of the solution, the cost and time to implement, the overall risk and whether any mitigations are applied in the interim. Generally, deficiencies should be resolved as soon as is reasonably possible.
  - ii) Isolated enduring exceptions encountered during implementation, such as unique equipment or environments (e.g., specialized manufacturing equipment or a unique laboratory environment) may prevent the implementation of certain security requirements. Isolated enduring exceptions are typically not suitable to address in plans of action, but when described, along with any mitigations, in the system security plan such exceptions should be assessed as 'implemented.'
- i) For certain requirements, questions often arise on whether or not they are actually implemented. These situations are addressed below:
  - i) Security Requirements 3.1.12, 3.1.16, 3.1.18: Companies commonly do not allow remote access, wireless access or connection of mobile devices and may indicate these requirements as 'Not Applicable' or 'Not Implemented' in the system security plan. The evaluator should not deduct points in such cases. However, if the company disallows use of remote, wireless, or mobile access, they should also have a policy and procedure in place to insure these capabilities are not enabled inadvertently. This should be discussed as part of the Medium-

Level assessment, and if such policy and procedures are not in place a point should be assessed.

- ii) Security Requirement 3.13.8: When implementing this requirement, encryption, though preferred, is not required if using common-carrier provided Multiprotocol Label Switching (MPLS), as the MPLS separation provides sufficient protection without encryption.
- iii) Security Requirement 3.13.11: Cryptography used to protect the confidentiality of CUI must be FIPS-validated, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient - the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. Note however, that this is required when encryption is required for protection, which is typically external to the contractor's covered information system (assuming the system meets NIST SP 800-171). Cryptography used for other purposes within the protected information system need not be FIPS validated. When required, if encryption is not employed (FIPS validated or otherwise), 5 points are subtracted from the score of 110. If encryption is employed, but is not FIPS validated, 3 points are subtracted from the score of 110. Isolated use of non-FIPS validated cryptography, with an associated Plan of Action, should be treated as a temporary deficiency and assessed as 'implemented.'
- j) If a contractor received a favorable adjudication from the DoD CIO indicating that a requirement is not applicable or that an alternative security measure is equally effective in accordance with DFARS 252.204-7008 or 7012, the DoD CIO assessment should be included in the Contractor's system security plan. Implemented security measures adjudicated by the DoD CIO as equally effective, and security requirements approved by the DoD CIO as 'not applicable,' will be assessed as 'implemented.' Once DOD CIO assessments approving "not applicable" requirements or "alternative security measures" are included in the Contractor's system security plan, the contractor does not need to submit that documentation for every current contract with the DFARS 252.204-7012 clause unless specifically requested to do so by the contracting officer. When completing the Basic (Contractor Self-Assessment) NIST SP 800-171 DoD Assessment Results Format, the contractor shall **score** any security requirements for which an assessment of "not applicable" or "alternative security measures" was previously approved by DoD CIO as 'implemented'.
- k) A template illustrating the application of this scoring methodology is provided at Annex A of this document.
- l) DoD will provide medium and high assessment results to the Contractor and offer the opportunity for rebuttal and adjudication of assessment results. Upon completion of



each assessment, the assessed contractor has 14 business days to provide additional information to the assessment team, to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

6) Documenting *NIST SP 800-171 DoD Assessment* Results

- a) A summary level score for basic assessments completed by the Contractor, and for medium and high assessments conducted by DoD, will be posted in the Supplier Performance Risk System (SPRS) to provide DoD Components with visibility to the results of strategic assessments.
  - i) SPRS is defined by DoD Instruction (DoDI) 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information, October 15, 2019 available at <https://www.esd.whs.mil/DD/>.
  - ii) SPRS is the authoritative source to retrieve supplier and product performance information for the DoD acquisition community to assess and monitor unclassified performance, and to assess corporate business practices related to DoD contracts and the supplier's management of risk.
- b) Assessment results posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI), available at <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?ver=2019-10-15-115609-957>. Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own results in accordance with the SPRS Software User's Guide for Awardees/Contractors available at [https://www.sprs.csd.disa.mil/pdf/SPRS\\_Awardee.pdf](https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf).
- c) A contractor may [post the results of their Basic Assessments conducted in accordance with Section 5 and Annex B of this document in SPRS \(via the Procurement Integrated Enterprise Environment \(PIEE\)\)](#).
- d) DoD will post the following Medium and/or High *NIST SP 800-171 DoD Assessment* results to SPRS for each system security plan assessed:
  - i) The standard assessed (e.g., NIST SP 800-171 Rev 1).
  - ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC) or Commercial and Government Entity (CAGE) Code).
  - iii) Each system security plan assessed, mapped to the specific industry CAGE code(s) associated with the information system(s) addressed by the system security plan. All corporate CAGE codes must be mapped to all appropriate

system security plan(s) if the contractor has more than one system security plan and CAGE code. Additionally, a brief description of the system security plan architecture may be required if more than one plan exists.

- iv) Date and level of the assessment, i.e., basic, medium, or high.
- v) Summary level score (e.g., 105 out of 110), but not the individual value assigned for each requirement.
- vi) Date a score of 110 is expected to be achieved (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.
- e) Department policy/procedures/guidance will be updated to direct acquisition/procurement officials and contractors to access SPRS to determine if a strategic assessment has been conducted.
- f) DoD Components should rely on assessment results posted in SPRS in lieu of including requirements to assess implementation of NIST SP 800-171 on a contract-by-contract basis.
- g) A High *NIST SP 800-171 DoD Assessment* may result in documentation in addition to that listed in 6) d) of this document. DoD will retain and protect any such documentation as For Official Use Only (FOUO) and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

## 7) Glossary of Terms

- a) Enduring exception. Remediation is not feasible; no plan of action required; must be documented within a system security plan.
- b) Temporary deficiency. Remediation of deficiency is feasible; known fix is in process; requires a plan of action. For the purposes of a DoD NIST SP 800-171 DoD Assessment, a 'temporary deficiency' is not based on an 'in progress' initial implementation of the requirement. A temporary deficiency arises after implementation. A Temporary deficiency may also apply during the initial implementation of a NIST SP 800-171 requirement if, during roll-out, specific issues with certain equipment is discovered that has to be separately addressed.

## Annex A - NIST SP 800-171 DoD Assessment Scoring Template

- The following template illustrates the scoring methodology described in Section 5. If all requirements are met, a score of 110 is awarded. For each requirement not met, the associated value is subtracted from 110. Consistency results from the fact that the assessments are based on what is not yet implemented, or document that all requirements have been met.
- It is important to note an assessment is about the extent to which the company has implemented the requirements. It is not a value judgement about the specific approach to implementing – in other words, all solutions that meet the requirements are acceptable. This is not an assessment of one solution compared to another.
- Scoring for Basic, Medium, and High *NIST SP 800-171 DoD Assessments* is the same.
- While NIST does not prioritize requirements in terms of impact, certain requirements do have more impact than others. In this scoring methodology security requirements are weighted based on their effect on the information system and DoD CUI created on or transiting that system.

### NIST SP 800-171 DoD Assessment Scoring Template

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

Security Requirement		Value	Comment
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1	
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	1	
3.1.11	Terminate (automatically) a user session after a defined condition.	1	
3.1.12	Monitor and control remote access sessions.	5	Do not subtract points if remote access not permitted
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	5	Do not subtract points if remote access not permitted
3.1.14	Route remote access via managed access control points.	1	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1	
3.1.16	Authorize wireless access prior to allowing such connections.	5	Do not subtract points if wireless access not permitted
3.1.17	Protect wireless access using authentication and encryption.	5	Do not subtract points if wireless access not permitted
3.1.18	Control connection of mobile devices.	5	Do not subtract points if connection of mobile devices is not permitted
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms	3	Exposure limited to CUI on mobile platform
3.1.20*	Verify and control/limit connections to and use of external systems.	1	
3.1.21	Limit use of portable storage devices on external systems.	1	
3.1.22*	Control CUI posted or processed on publicly accessible systems.	1	
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	5	

Security Requirement		Value	Comment
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	5	
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1	
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	5	
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3	
3.3.3	Review and update logged events.	1	
3.3.4	Alert in the event of an audit logging process failure.	1	
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	5	
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	1	
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	1	
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1	
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1	
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	5	

Security Requirement		Value	Comment
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	5	
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	1	
3.4.4	Analyze the security impact of changes prior to implementation.	1	
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5	
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	5	
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	5	
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	5	
3.4.9	Control and monitor user-installed software.	1	
3.5.1*	Identify system users, processes acting on behalf of users, and devices.	5	
3.5.2*	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5	
3.5.3	Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	3 to 5	Subtract 5 points if MFA not implemented. Subtract 3 points if implemented for remote and privileged users, but not the general user
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1	
3.5.5	Prevent reuse of identifiers for a defined period.	1	
3.5.6	Disable identifiers after a defined period of inactivity.	1	

Security Requirement		Value	Comment
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1	
3.5.8	Prohibit password reuse for a specified number of generations.	1	
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1	
3.5.10	Store and transmit only cryptographically-protected passwords.	5	Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords
3.5.11	Obscure feedback of authentication information.	1	
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	5	
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	5	
3.6.3	Test the organizational incident response capability.	1	
3.7.1	Perform maintenance on organizational systems.	3	
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5	
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	1	
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3	
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5	

Security Requirement		Value	Comment
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	1	
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3	Exposure limited to CUI on media
3.8.2	Limit access to CUI on system media to authorized users.	3	Exposure limited to CUI on media
3.8.3*	Sanitize or destroy system media containing CUI before disposal or release for reuse.	5	While exposure limited to CUI on media, failure to sanitize can result in continual exposure of CUI
3.8.4	Mark media with necessary CUI markings and distribution limitations.	1	
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	1	
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	1	
3.8.7	Control the use of removable media on system components.	5	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	1	
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3	
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	5	
3.10.1*	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5	
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	5	



Security Requirement		Value	Comment
3.10.3*	Escort visitors and monitor visitor activity.	1	
3.10.4*	Maintain audit logs of physical access.	1	
3.10.5*	Control and manage physical access devices.	1	
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1	
3.11.1	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 CUI.	3	
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	5	
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	1	
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	5	
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3	
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	5	
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	NA	The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'
3.13.1*	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	5	

Security Requirement		Value	Comment
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	5	
3.13.3	Separate user functionality from system management functionality.	1	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	1	
3.13.5*	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	5	
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	5	
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	1	
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3	
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	1	
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	1	
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	3 to 5	Subtract 5 points if no cryptography is employed; 3 points if mostly not FIPS validated
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	1	

Security Requirement		Value	Comment
3.13.13	Control and monitor the use of mobile code.	1	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1	
3.13.15	Protect the authenticity of communications sessions.	5	
3.13.16	Protect the confidentiality of CUI at rest.	1	
3.14.1*	Identify, report, and correct system flaws in a timely manner.	5	
3.14.2*	Provide protection from malicious code at designated locations within organizational systems.	5	
3.14.3	Monitor system security alerts and advisories and take action in response.	5	
3.14.4*	Update malicious code protection mechanisms when new releases are available.	5	
3.14.5*	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3	
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	5	
3.14.7	Identify unauthorized use of organizational systems	3	

\* Basic safeguarding requirements and procedures to protect covered contractor information systems per Federal Acquisition Regulation (FAR) clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

## Annex B - Basic (Contractor Self-Assessment) NIST SP 800-171 DoD Assessment Results Format

- Score your implementation of the security requirements in NIST SP 800-171 based on Section 5 and Annex A of this document.
- Document your Basic (self) NIST SP 800-171 DoD Assessment score in Supplier Performance Risk System (SPRS). A Procurement Integrated Enterprise Environment (PIEE) account with a SPRS “Cyber Vendor” role will be required to enter Basic Assessment information into SPRS. This role may be requested through PIEE.
- Information required for entering results of a Basic NIST SP 800-171 DoD Assessment into SPRS include:
  - Date of the assessment
  - Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement)
  - Scope of the Basic Assessment - Identify each system security plan (security requirement 3.12.4) supporting the performance of this contract. All company CAGE codes must be mapped to the appropriate system security plan(s). Additionally, a brief description of the plan architecture may be required, if more than one plan exists.
    - Select Open CAGE Hierarchy to choose CAGEs covered by the system security plan.
    - Note: if a CAGE does not appear in the hierarchy, update your company’s records in the System for Award Management (SAM); ensure immediate/highest level owner CAGEs are correctly indicated. SPRS will normally be updated within 24 hours.
  - Plan of Action Completion Date – date that a score of 110 is expected to be achieved for each system security plan assessed (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171 (security requirement 3.12.2).
- Informational links include:
  - PIEE Landing Page: <https://wawf.eb.mil/piee-landing/>
  - Information on requesting access via PIEE may be found here: <https://www.sprs.csd.disa.mil/access.htm>
  - Information on entering Cyber assessment scores into SPRS may be found here: <https://www.sprs.csd.disa.mil/reference.htm>
  - SPRS Homepage: <https://www.sprs.csd.disa.mil/default.htm>