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

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

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#252.204-7012.

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.

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.SP.800-171r1.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.

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.

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 internal information system clock synchronization

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 pf 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 dimished 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 allowindividuals 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., smart phones, 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, employee,s 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 though 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
- 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 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 mailattachments, 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 typicallyimplemented 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