CMMC Assessment Guide

Level 2

Version 2.0 | December 2021

NOTICES

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center, and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory LLC, a University Affiliated Research Center.

TABLE OF CONTENTS

This page intentionally left blank.

Introduction

This document provides assessment guidance for conducting Cybersecurity Maturity Model Certification (CMMC) assessments for Level 2. The CMMC levels and the associated set of practices are cumulative. More specifically, in order for a Defense Industrial Base (DIB) contractor to achieve CMMC Level 2 certification, it must demonstrate achievement of all Level 1 and Level 2 practices. Guidance for conducting a CMMC Level 1 self-assessment can be found in *CMMC Self-Assessment Guide – Level 1*. Guidance for conducting a CMMC Level 3 assessment will be published at a later date. More details on the model can be found in the *CMMC Model Overview* document.

A CMMC assessment is the methodology to certify that a contractor is compliant with the CMMC Level 2 standard. Contractors requiring a CMMC Level 2 certification must have a CMMC Level 2 assessment conducted by CMMC Third-Party Assessment Organization (C3PAO) and Certified Assessor. DIB contractors using this guide to perform CMMC Level 2 self-assessment, will not result in a CMMC Level 2 certification.

CMMC Level Descriptions

CMMC Levels 1 and 2 consist of the security requirements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

CMMC Level 1 addresses the protection of Federal Contract Information (FCI) and encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21, which defines FCI as:

> *Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.*

CMMC Level 2 addresses the protection of Controlled Unclassified Information (CUI), which the National Archives and Record Administration (NARA) defines as:

> *Information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.*

For a CMMC Level 2 assessment, the practices that encompass CMMC Levels 1 and 2, for the protection of CUI, apply. CMMC Level 2 provides increased assurance to the DoD that a contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow with its subcontractors in a multi-tier supply chain.

Purpose and Audience

This guide is intended for Certified Assessors, contractors, as well as information technology (IT) and cybersecurity professionals who secure data and systems with responsibilities for information risk management and governance, system development, security assessment and monitoring, and security implementation and operations. Contractors can use this document to prepare for a CMMC assessment to include but not limited to a self-assessment.

Document Organization

This document is organized into the following sections:

- **Assessment and Certification:** provides an overview of the CMMC assessment and certification process, guidance around contractor size, and the assessment scope.
- **Assessment Criteria and Methodology:** provides guidance on the criteria and methodology (i.e., *interview*, *examine*, and *test*) Certified Assessors will employ during a CMMC assessment, as well as practice findings.
- **CMMC-Specific Terms:** provides clarification of the intent and scope of specific terms as used in the context of CMMC.
- **Practice Descriptions:** provides the assessment requirements and specifics for each CMMC practice.

Assessment and Certification

Certified Assessors will use the assessment methods as defined in this guide to conduct CMMC Level 2 assessments. Certified Assessors will review information and evidence to independently verify that a contractor meets the stated assessment objectives for all of the required practices.

A contractor can achieve a CMMC certification for an entire enterprise network, for particular segment(s), or for a specific enclave, depending upon how the CMMC assessment is scoped.

Contractor Size

The CMMC assessment methodology follows a data-centric security process that applies the practices equally, regardless of the contractor's size, constraints, or complexity. All CMMC levels are achievable by small, medium, and large contractors.

Assessment Scope

Prior to conducting a CMMC assessment, the contractor must specify the CMMC Assessment Scope. The CMMC Assessment Scope informs which assets within the contractor's environment will be assessed and the details of the assessment. To specify the CMMC Assessment Scope, contractors will map their assets into one of the following five categories: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets.

Table 1 provides an overview of these asset categories and the contractor requirements and assessment implications. *CMMC Assessment Scope – Level 2* provides additional detailed guidance on the CMMC Assessment Scope.

Table 1. CMMC Asset Categories Overview

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Assets that are in the CMMC Assessment Scope			
CUI Assets	• Assets that process, store, or transmit CUI	• Document in the asset inventory • Document in the System Security Plan (SSP) • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC practices	• Assess against CMMC practices
Security Protection Assets	• Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI		

Contractor Risk Managed Assets	• Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
	• Assets are not required to be physically or logically separated from CUI assets
		• Document in the asset inventory
		• Document in the SSP
		  ○ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices
		• Document in the network diagram of the CMMC Assessment Scope
			• Review the SSP in accordance with practice CA.L2-3.12.4
			  ○ If appropriately documented, do not assess against other CMMC practices
			  ○ If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks
			  ○ The limited spot check(s) shall not materially increase the assessment duration nor the assessment cost
			  ○ The limited spot check(s) will be within the defined Assessment Scope

Specialized Assets	• Assets that may or may not process, store, or transmit CUI • Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment		• Review the SSP in accordance with practice CA.L2-3.12.4 • Do not assess against other CMMC practices
Assets that are not in the CMMC Assessment Scope			
Out-of-Scope Assets	• Assets that cannot process, store, or transmit CUI	• Assets are required to be physically or logically separated from CUI assets	• None

CMMC-Specific Terms

The CMMC framework has specific terms that align with its practices. While some terms may have other definitions in open forums and within NIST documentation, it is important for contractors, users, and assessors to understand the meaning of these terms as they apply to the CMMC framework. These definitions and sources also appear in the *CMMC Glossary and Acronyms;* they are repeated here for emphasis as it is important to know the specific definition intended by CMMC when interpreting the practices presented later in the document.

The specific terms as associated with CMMC Levels 1 and 2 are:

- **Assessment:** The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization [NIST SP 800-37 Rev. 2]. *Assessment* is the term used by CMMC for the activity performed by the C3PAO to evaluate the CMMC level of a DIB contractor. *Self-assessment* is the term used by CMMC for the activity performed by a DIB contractor to evaluate their own CMMC level.
- **Asset (Organizational Asset):** Anything that has value to an organization, including, but not limited to, another organization, person, computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards) [NISTIR 7693, NISTIR 7694]. Understanding *assets* is critical to identifying the *CMMC Assessment Scope*; for more information see *CMMC Assessment Scope – Level 2*.
- **CMMC Assessment Scope:** Includes all *assets* in the contractor's environment that will be assessed [CMMC].
- **Event:** Any observable occurrence in a system and/or network. *Events* sometimes provide indication that an *incident* is occurring [CNSSI 4009].
- **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 [NIST SP 800-171 Rev 2].
- **Monitor:** The act of continually checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected at an *organizationally defined* frequency and rate [NIST SP 800-160 (adapted)].
- **Organizationally Defined:** As determined by the contractor being assessed. This can be applied to a frequency or rate at which something occurs within a given time period, or it could be associated with describing the configuration of a contractor's solution [CMMC].

- **Periodically:** Occurring at regular intervals [Oxford Dictionary (adapted)]. As used in many practices within CMMC, the interval length is *organizationally defined* to provided contractor flexibility, with an interval length of no more than one year.

Assessment Criteria and Methodology

The *CMMC Assessment Guide – Level 2* leverages the assessment procedure described in NIST SP 800-171A Section 2.1[1]:

> *An assessment procedure consists of an assessment objective and a set of potential assessment methods and assessment objects that can be used to conduct the assessment. Each assessment objective includes a determination statement related to the [CMMC practice] that is the subject of the assessment. The determination statements are linked to the content of the [CMMC practice] to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to a [CMMC practice] produces assessment findings. These findings reflect, or are subsequently used, to help determine if the [CMMC practice] has been satisfied.*
>
> *Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals.*
>
> - *Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system.*
> - *Mechanisms are the specific hardware, software, or firmware safeguards employed within a system.*
> - *Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic).*
> - *Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.*
>
> *The assessment methods define the nature and the extent of the assessor's actions. The methods include* examine, interview, *and* test.
>
> - *The* examine *method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the* examine *method is to facilitate understanding, achieve clarification, or obtain evidence.*
> - *The* interview *method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.*
> - *And finally, the* test *method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior.*

[1] NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*, July 2018.

> *In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.*

The guidance specified in NIST SP 800-171A focuses on CUI. Because CMMC Level 1 focuses on safeguarding FCI, the applicable assessment objectives for Level 1 are updated to address FCI. These practices also apply to CMMC Level 2 assessments where the contractor has CUI because CMMC is cumulative.

Criteria

Assessment objectives are provided for each practice and are based on existing criteria from NIST SP 800-171A. The criteria are authoritative and provide a basis for a CMMC Certified Assessor to conduct an assessment of a practice.

Methodology

During the CMMC assessment, the Certified Assessor will verify and validate that the contractor has properly implemented the practices. Because a contractor can meet the assessment objectives in different ways (e.g., through documentation, computer configuration, network configuration, or training) the Certified Assessor may use a variety of techniques, including any of the three assessment methods described above from NIST SP 800-171A, to determine if the contractor meets the intent of the practices.

The Certified Assessor will follow the guidance in NIST SP 800-171A when determining which assessment methods to use:

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

The primary deliverable of an assessment is a report that contains the findings associated with each practice. For more detailed information on assessment methods, see Appendix D of NIST SP 800-171A.

Who Is Interviewed

The Certified Assessor has discussions with contractor staff to understand if a practice has been addressed. Interviews of applicable staff (possibly at different organizational levels) determine if CMMC practices are implemented as well as if adequate resourcing, training, and planning have occurred for individuals to perform the practices.

What Is Examined

Examination includes reviewing, inspecting, observing, studying, or analyzing assessment objects. The objects can be documents, mechanisms, or activities.

For some practices, the Certified Assessor reviews documentation to determine if assessment objectives are met. Interviews with contractor staff may identify the documents the contractor uses. Documents need to be in their final forms; working papers (e.g., drafts) of documentation are not eligible to be submitted as evidence because they are not yet official and are still subject to change. Common types of documents that can be used as evidence include:

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system-level, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive. A contractor may not have these specific documents, and other documents may be used to provide evidence of compliance.

In other cases, the practice is best assessed by observing that safeguards are in place by viewing hardware or associated configuration information or observing staff following a process.

What Is Tested

Testing is an important part of the assessment process. Interviews tell the Certified Assessor what the contractor staff believe to be true, documentation provides evidence of intent, and testing demonstrates what has or has not been done. For example, contractor staff may talk about how users are identified; documentation may provide details on how users are identified, but seeing a demonstration of identifying users provides evidence that the practice is met. The Certified Assessor will determine which practices or objectives within a practice need demonstration or testing. Not all practices will require testing.

Assessment Findings

The assessment of a CMMC practice results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE. To achieve a specific CMMC level, the contractor will need a finding of MET or NOT APPLICABLE finding on all CMMC practices required for the desired level as well as for all lower levels. For example, a contractor will need a MET or NOT APPLICABLE finding on all CMMC practices at Levels 2 and 1 to achieve a CMMC Level 2 certification.

- **MET**: The contractor successfully meets the practice. For each practice marked MET, the Certified Assessor includes statements that indicate the response conforms to all objectives and documents the appropriate evidence to support the response.

- **NOT MET**: The contractor has not met the practice. For each practice marked NOT MET, the Certified Assessor includes statements that explain why and documents the appropriate evidence that the contractor does not conform fully to all of the objectives.
- **NOT APPLICABLE (N/A)**: The practice does not apply for the assessment. For each practice marked N/A, the Certified Assessor includes a statement that explains why the practice does not apply to the contractor. For example, SC.L1-3.13.5 might be N/A if there are no publicly accessible systems.

A contractor can inherit practice objectives. A practice objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. An ESP may be external people, technology, or facilities that the contractor uses, including cloud service providers, managed service providers, managed security service providers, cybersecurity-as-a-service providers.

Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met. For each practice objective that is inherited, the Certified Assessor includes statements that indicate how they were evaluated and from whom they are inherited. If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a NOT MET for the practice.

Practice Descriptions

This section provides detailed information for assessing each CMMC practice beyond what is provided in the *CMMC Model Overview* document. The section is organized by domain (DD), level (L), and then practices (REQ). Practices by level are presented in the order in which they appear in the *CMMC Model Matrix* from top to bottom, not numerical order. Each practice description contains the following elements:

- **Practice Number, Name, and Statement:** Headed by the practice identification number in the format, DD.L#-REQ (e.g., AC.L1-3.1.1); followed by the practice short name identifier, meant to be used for quick reference only; and finally followed by the complete CMMC practice statement.
- **Assessment Objectives [SOURCE]:** Identifies the specific list of objectives that must be met to receive MET for the practice as defined in NIST SP 800-171A.
- **Potential Assessment Methods and Objects [SOURCE]:** Defines the nature and the extent of the Certified Assessor's actions. Potential assessment methods and objects are as defined in NIST SP 800-171A. The methods include *examine*, *interview*, and *test*. Assessment objects identify the items being assessed and can include specifications, mechanisms, activities, and individuals.
- **Discussion [NIST SP 800-171 R2]:** Contains discussion from the associated NIST SP 800-171 security requirement. CMMC Level 1 aligns with FAR Clause 52.204-21, which focuses on FCI, and the NIST text has been modified to reflect this.
- **Further Discussion:**
    - Expands upon the NIST content to provide more information on the practice intent.
    - Contains examples illustrating how the staff of contractors might apply the practices. These examples provide insight, but are not intended to be prescriptive of how the practice must be implemented, nor comprehensive of all assessment objectives necessary to achieve the practice. The assessment objectives met within the example are referenced by letter in a bracket (e.g., [a,d] for objectives "a" and "d") within the text. Note that some of the examples contain fictitious company names; all company names used in this document are fictitious.
    - Provides potential assessment considerations. These may include common considerations for assessing the practice and potential questions a Certified Assessor may ask when assessing the objectives, including, in some cases, questions from NIST Handbook 162[2].
- **Key References:** Lists the related basic safeguarding requirement from FAR Clause 52.204-21 (Level 1 only) and the security requirement from NIST SP 800-171 Rev 2. The *CMMC Model Overview, Appendix B: Source Mapping* provides additional references.

[2] NIST Handbook 162, *NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, November 2017.

Access Control (AC)

Level 1 AC Practices

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

DISCUSSION [NIST SP 800-171 R2]

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses *[sic]* non-privileged) are addressed in requirement 3.1.2 (AC.L1-3.1.2).

FURTHER DISCUSSION

Identify users, processes, and devices that are allowed to use company computers and can log on to the company network. Automated updates and other automatic processes should be associated with the user who initiated (authorized) the process. Limit the devices (e.g., printers) that can be accessed by company computers. Set up your system so that only authorized users, processes, and devices can access the company network.

This practice, AC.L1-3.1.1, controls system access based on user, process, or device identity. AC.L1-3.1.1 leverages IA.L1-3.5.1 which provides a vetted and trusted identity for access control.

Example 1

Your company maintains a list of all personnel authorized to use company information systems [a]. This list is used to support identification and authentication activities conducted by IT when authorizing access to systems [a,d].

Example 2

A coworker wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network and will prevent network access by unauthorized systems and devices [c]. You help the coworker submit a ticket that asks for the printer to be granted access to the network, and appropriate leadership approves the device [f].

Potential Assessment Considerations

- Is a list of authorized users maintained that defines their identities and roles [a]?
- Are account requests authorized before system access is granted [d,e,f]?[3]

KEY REFERENCES

- FAR Clause 52.204-21 b.1.i
- NIST SP 800-171 Rev 2 3.1.1

[3] NIST Handbook 162 Section 3.1.1

AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[b] system access is limited to the defined types of transactions and functions for authorized users.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing access control policy].

DISCUSSION [NIST SP 800-171 R2]

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

FURTHER DISCUSSION

Limit users to only the information systems, roles, or applications they are permitted to use and are needed for their roles and responsibilities. Limit access to applications and data

based on the authorized users' roles and responsibilities. Common types of functions a user can be assigned are create, read, update, and delete.

Example

You supervise the team that manages DoD contracts for your company. Members of your team need to access the contract information to perform their work properly. Because some of that data contains FCI, you work with IT to set up your group's systems so that users can be assigned access based on their specific roles [a]. Each role limits whether an employee has read-access or create/read/delete/update -access [b]. Implementing this access control restricts access to FCI information unless specifically authorized.

Potential Assessment Considerations

- Are access control lists used to limit access to applications and data based on role and/or identity [a]?[4]
- Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools) [b]?[5]

KEY REFERENCES

- FAR Clause 52.204-21 b.1.ii
- NIST SP 800-171 Rev 2 3.1.2

[4] NIST Handbook 162 Section 3.1.2
[5] NIST Handbook 162 Section 3.1.2

AC.L1-3.1.20 – EXTERNAL CONNECTIONS

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] connections to external systems are identified;

[b] the use of external systems is identified;

[c] connections to external systems are verified;

[d] the use of external systems is verified;

[e] connections to external systems are controlled/limited; and

[f] the use of external systems is controlled/limited.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing the use of external systems; terms and conditions for external systems; system security plan; list of applications accessible from external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing terms and conditions on use of external systems].

DISCUSSION [NIST SP 800-171 R2]

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of FCI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of FCI across an organization, the organization may have systems that process FCI and others that do not. And among the systems that process FCI there are likely access restrictions for FCI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

FURTHER DISCUSSION

Control and manage connections between your company network and outside networks. Outside networks could include the public internet, one of your own company's networks that falls outside of your CMMC Assessment Scope (e.g., an isolated lab), or a network that does not belong to your company. Tools to accomplish include firewalls and connection allow/deny lists. External systems not controlled by your company could be running applications that are prohibited or blocked. Control and limit access to corporate networks from personally owned devices such as laptops, tablets, and phones. You may choose to limit how and when your network is connected to outside systems or only allow certain employees to connect to outside systems from network resources.

Example

You and your coworkers are working on a big proposal and will put in extra hours over the weekend to get it done. Part of the proposal includes FCI. Because FCI should not be shared publicly, you remind your coworkers of the policy requirement to use their company laptops, not personal laptops or tablets, when working on the proposal over the weekend [b,f]. You also remind everyone to work from the cloud environment that is approved for processing and storing FCI rather than the other collaborative tools that may be used for other projects [b,f].

Potential Assessment Considerations

- Are all connections to external systems outside of the assessment scope identified [a]?

- Are external systems (e.g., systems managed by contractors, partners, or vendors; personal devices) that are permitted to connect to or make use of organizational systems identified [b]?
- Are methods employed to ensure that only authorized connections are being made to external systems (e.g., requiring log-ins or certificates, access from a specific IP address, or access via Virtual Private Network (VPN)) [c,e]?
- Are methods employed to confirm that only authorized external systems are connecting (e.g., if employees are receiving company email on personal cell phones, is the contractor checking to verify that only known/expected devices are connecting) [d]?
- Is the use of external systems limited, including by policy or physical control [f]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.iii
- NIST SP 800-171 Rev 2 3.1.20

AC.L1-3.1.22 – CONTROL PUBLIC INFORMATION

Control information posted or processed on publicly accessible information systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] individuals authorized to post or process information on publicly accessible systems are identified;

[b] procedures to ensure FCI is not posted or processed on publicly accessible systems are identified;

[c] a review process is in place prior to posting of any content to publicly accessible systems;

[d] content on publicly accessible systems is reviewed to ensure that it does not include FCI; and

[e] mechanisms are in place to remove and address improper posting of FCI.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing publicly accessible content; system security plan; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs and records; security awareness training records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing management of publicly accessible content].

DISCUSSION [NIST SP 800-171 R2]

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, FCI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post FCI onto publicly accessible

systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

FURTHER DISCUSSION

Do not allow FCI to become public – always safeguard the confidentiality of FCI by controlling the posting of FCI on company-controlled websites or public forums, and the exposure of FCI in public presentations or on public displays. It is important to know which users are allowed to publish information on publicly accessible systems, like your company website, and implement a review process before posting such information. If FCI is discovered on a publicly accessible system, procedures should be in place to remove that information and alert the appropriate parties.

Example

Your company decides to start issuing press releases about its projects in an effort to reach more potential customers. Your company receives FCI from the government as part of its DoD contract. Because you recognize the need to manage controlled information, including FCI, you meet with the employees who write the releases and post information to establish a review process [c]. It is decided that you will review press releases for FCI before posting it on the company website [a,d]. Only certain employees will be authorized to post to the website [a].

Potential Assessment Considerations

- Does information on externally facing systems (i.e., publicly accessible) have a documented approval chain for public release [c]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.iv
- NIST SP 800-171 Rev 2 3.1.22

Level 2 AC Practices

AC.L2-3.1.3 – CONTROL CUI FLOW

Control the flow of CUI in accordance with approved authorizations.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] information flow control policies are defined;

[b] methods and enforcement mechanisms for controlling the flow of CUI are defined;

[c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified;

[d] authorizations for controlling the flow of CUI are defined; and

[e] approved authorizations for controlling the flow of CUI are enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

DISCUSSION [NIST SP 800-171 R2]

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: 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 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.

Organizations commonly use 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 systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict 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). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST SP 800-41 provides guidance on firewalls and firewall policy. SP 800-125B provides guidance on security for virtualization technologies.

In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes: 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 labels.

FURTHER DISCUSSION

Typically, companies will have a firewall between the internal network and the internet. Often multiple firewalls or routing switches are used inside a network to create zones to separate sensitive data, business units, or user groups. Proxy servers can be used to break the connection between multiple networks. All traffic entering or leaving a network is intercepted by the proxy, preventing direct access between networks. Companies should also ensure by policy and enforcement mechanisms that all CUI allowed to flow across the internet is encrypted.

Example 1

As a system administrator, you configure a proxy device on your company's network. Your goal is to better mask and protect the devices inside the network while enforcing information flow policies. After the device is configured, information does not flow directly from the

internal network to the internet. The proxy device intercepts the traffic and analyzes it to determine if the traffic conforms to organization information flow control policies. If it does, the device allows the information to pass to its destination [b]. The proxy blocks traffic that does not meet policy requirements [e].

Example 2

As a subcontractor on a DoD contract, your organization sometimes needs to transmit CUI to the prime contractor. You create a policy document that specifies who is allowed to transmit CUI and that such transmission requires manager approval [a,c,d]. The policy instructs users to encrypt any CUI transmitted via email or to use a designated secure file sharing utility [b,d]. The policy states that users who do not follow appropriate procedures may be subject to disciplinary action [e].

Potential Assessment Considerations

- Are designated sources of regulated data identified within the system (e.g., internal network and IP address) and between interconnected systems (e.g., external networks, IP addresses, ports, and protocols) [c]?
- Are designated destinations of regulated data identified within the system (e.g., internal network and IP address) and between interconnected systems (external networks and IP addresses) [c]?
- Are authorizations defined for each source and destination within the system and between interconnected systems (e.g., allow or deny rules for each combination of source and destination) [d]?
- Are approved authorizations for controlling the flow of regulated data enforced within the system and between interconnected systems (e.g., traffic between authorized sources and destinations is allowed and traffic between unauthorized sources and destinations is denied) [e]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.3

AC.L2-3.1.4 – SEPARATION OF DUTIES

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the duties of individuals requiring separation are defined;

[b] responsibilities for duties that require separation are assigned to separate individuals; and

[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms implementing separation of duties policy].

DISCUSSION [NIST SP 800-171 R2]

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

FURTHER DISCUSSION

No one person should be in charge of an entire critical task from beginning to end. Documenting and dividing elements of important duties and tasks between employees reduces intentional or unintentional execution of malicious activities.

Example 1

You are responsible for the management of several key systems within your organization. You assign the task of reviewing the system logs to two different people. This way, no one person is solely responsible for the execution of this critical security function [c].

Example 2

You are a system administrator. Human Resources notifies you of a new hire, and you create an account with general privileges, but you are not allowed to grant access to systems that contain CUI [a,b]. The program manager contacts the team in your organization that has system administration authority over the CUI systems and informs them which CUI the new hire will need to access. Subsequently, a second system administrator grants access privileges to the new hire [c].

Potential Assessment Considerations

- Does system documentation identify the system functions or processes that require separation of duties (e.g., function combinations that represent a conflict of interest or an over-allocation of security privilege for one individual) [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.4

AC.L2-3.1.5 – LEAST PRIVILEGE

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] privileged accounts are identified;

[b] access to privileged accounts is authorized in accordance with the principle of least privilege;

[c] security functions are identified; and

[d] access to security functions is authorized in accordance with the principle of least privilege.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring/audit records; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access is to be explicitly authorized; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities; personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management; mechanisms implementing least privilege functions; mechanisms prohibiting privileged access to the system].

DISCUSSION [NIST SP 800-171 R2]

Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational

missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

FURTHER DISCUSSION

The principle of least privilege applies to all users and processes on all systems, but it is critical to systems containing or accessing CUI. Least privilege:

- restricts user access to only the machines and information needed to fulfill job responsibilities; and
- limits what system configuration settings users can change, only allowing individuals with a business need to change them.

Example

As a system administrator, you create accounts. By default, everyone is assigned a basic user role, which prevents a user from modifying system configurations. Privileged access is only assigned to users and processes that require it to carry out job functions, such as IT staff, and is very selectively granted [b,d].

Potential Assessment Considerations

- Are privileged accounts documented and is when they may be used defined [a]?
- Are users assigned privileged accounts to perform their job functions only when it is necessary [b]?
- Are necessary security functions identified (e.g., access control configuration, system configuration settings, or privileged account lists) that must be managed through the use of privileged accounts [c]?
- Is access to privileged functions and security information restricted to authorized employees [d]?[6]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.5

[6] NIST Handbook 162 Section 3.1.5

AC.L2-3.1.6 – NON-PRIVILEGED ACCOUNT USE

Use non-privileged accounts or roles when accessing nonsecurity functions.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] nonsecurity functions are identified; and

[b] users are required to use non-privileged accounts or roles when accessing nonsecurity functions.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing least privilege; system security plan; list of system-generated security functions assigned to system accounts or roles; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for defining least privileges necessary to accomplish specified organizational tasks; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms implementing least privilege functions].

DISCUSSION [NIST SP 800-171 R2]

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations 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 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.

FURTHER DISCUSSION

A user with a privileged account can perform more tasks and access more information than a person with a non-privileged account. Tasks (including unauthorized tasks orchestrated by attackers) performed when using the privileged account can have a greater impact on the system. System administrators and users with privileged accounts must be trained not to use their privileged accounts for everyday tasks, such as browsing the internet or connecting unnecessarily to other systems or services.

Example

You are a system administrator logged in using your privileged account and you need to look up how to reset a non-functioning application. You should log on to another computer with your non-privileged account before you connect to the web and start searching for the reset information [b]. That way, if your account is compromised during the search, it will be your regular user account rather than an account with elevated privileges.

Potential Assessment Considerations

- Are nonsecurity functions and non-privileged roles defined [a,b]?
- Is it required that nonsecurity functions only be accessed with the use of non-privileged accounts? How is this verified [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.6

AC.L2-3.1.7 – PRIVILEGED FUNCTIONS

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] privileged functions are defined;

[b] non-privileged users are defined;

[c] non-privileged users are prevented from executing privileged functions; and

[d] the execution of privileged functions is captured in audit logs.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing least privilege functions for non-privileged users; mechanisms auditing the execution of privileged functions].

DISCUSSION [NIST SP 800-171 R2]

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2 (AC.L1-3.1.2).

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

FURTHER DISCUSSION

Non-privileged users should receive only those permissions required to perform their basic job functions. Privileged users are granted additional permissions because their jobs require them. Privileged functions typically involve the control, monitoring, or administration of the system and its security measures. When these special privileged functions are performed, the activity must be captured in an audit log, which can be used to identify abuse. Non-privileged employees must not be granted permission to perform any of the functions of a privileged user.

This practice, AC.L2-3.1.7, manages non-privileged users by logging any attempts to execute privileged functions. AC.L2-3.1.7 leverages AU.L2-3.3.2, which ensures logging and traceability of user actions. AC.L2-3.1.7 also extends AC.L1-3.1.2, which defines a requirement to limit types of transactions and functions to those that authorized users are permitted to execute.

Example

As a system administrator for your organization, you have put security controls in place that prevent non-privileged users from performing privileged activities [a,b,c]. However, you accidentally gave a standard user elevated system administrator privileges. The organization has implemented an endpoint detection and response solution that provides visibility into the use of privileged activities. The monitoring system logs a security misconfiguration because the use of administrative privileges was performed by a user who was not known to have that ability. This allows you to correct the error [d].

Potential Assessment Considerations

- Is it possible to identify who enabled privileges at any particular time [d]?
- Are the privileged system functions documented (e.g., functions that involve the control, monitoring or administration of the system, including security functions and log management) [a]?
- Do documented procedures describe the configuration of the system to ensure system roles do not grant non-privileged users the ability to execute privileged functions [c]?
- Do procedures describe the configuration of system settings to capture the execution of all privileged functions in audit logs [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.7

AC.L2-3.1.8 – UNSUCCESSFUL LOGON ATTEMPTS

Limit unsuccessful logon attempts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the means of limiting unsuccessful logon attempts is defined; and

[b] the defined means of limiting unsuccessful logon attempts is implemented.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; system developers; system or network administrators].

Test

[SELECT FROM: Mechanisms implementing access control policy for unsuccessful logon attempts].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

FURTHER DISCUSSION

Consecutive unsuccessful logon attempts may indicate malicious activity. Contractors can mitigate these attacks by limiting the number of unsuccessful logon attempts, typically by locking the account. A defined number of consecutive unsuccessful logon attempts is a common configuration setting. Contractors are expected to set this number at a level that fits their risk profile with the knowledge that fewer unsuccessful attempts provide higher security.

After an unsuccessful login attempt threshold is exceeded and the system locks an account, the account may either remain locked until an administrator takes action to unlock it, or it may be locked for a predefined time after which it unlocks automatically.

Example

You attempt to log on to your work computer. You mistype your password three times in a row, and an error message is generated telling you the account is locked [b]. You call your IT help desk or system administrator to request assistance. The system administrator explains that the account is locked as a result of three unsuccessful logon attempts [a]. The administrator offers to unlock the account and notes that you can wait 30 minutes for the account to unlock automatically.

Potential Assessment Considerations

- Is there a defined threshold for the number of unsuccessful logon attempts for which the system takes action to prevent additional attempts [a]?
- Is a mechanism for limiting the number of unsuccessful logon attempts implemented and does it use the defined threshold [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.8

AC.L2-3.1.9 – PRIVACY & SECURITY NOTICES

Provide privacy and security notices consistent with applicable CUI rules.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category; and

[b] privacy and security notices are displayed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers].

Test

[SELECT FROM: Mechanisms implementing system use notification].

DISCUSSION [NIST SP 800-171 R2]

System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational 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. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

FURTHER DISCUSSION

Every system containing or providing access to CUI has legal requirements concerning user privacy and security notices. One method of addressing this requirement is the use of a

system-use notification banner that displays the legal requirements of using the system. Users may be required to click to agree to the displayed requirements of using the system each time they log on to the machine. This agreement can be used in the civil and/or criminal prosecution of an attacker that violates the terms.

The legal notification should meet all applicable requirements. At a minimum, the notice should inform the user that:

- information system usage may be monitored or recorded, and is subject to audit;
- unauthorized use of the information systems is prohibited;
- unauthorized use is subject to criminal and civil penalties;
- use of the information system affirms consent to monitoring and recording;
- the information system contains CUI with specific requirements imposed by the Department of Defense; and
- use of the information system may be subject to other specified requirements associated with certain types of CUI such as Export Controlled information.

Example

You are setting up IT equipment including a database server that will contain CUI. You have worked with legal counsel to draft a notification. It contains both general and specific CUI security and privacy requirements [a]. The system displays the required security and privacy information before anyone logs on to your organization's computers that contain or provide access to CUI [b].

For more information on CUI, refer to https://www.dodcui.mil/.

Potential Assessment Considerations

- Are requirements identified for privacy and security notices, and do the implemented practices match those identified requirements [a,b]? Discrepancies may indicate a deficient process and/or an incomplete practice.
- Are there any special requirements associated with the specific CUI category [a]?
- Are appropriate notices displayed in areas where paper-based CUI is stored and processed [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.9

AC.L2-3.1.10 – SESSION LOCK

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the period of inactivity after which the system initiates a session lock is defined;

[b] access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; and

[c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing access control policy for session lock].

DISCUSSION [NIST SP 800-171 R2]

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

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

FURTHER DISCUSSION

Session locks can be initiated by the user or, more fundamentally, enabled automatically when the system has been idle for a period of time, for example, five minutes. Session locks are a quick way to prevent unauthorized use of the systems without having a user log off. Minimum configuration requirements are left up to the organization to define.

A locked session shows pattern-hiding information on the screen to mask the data on the display.

Example

You are a system administrator. You notice that employees leave their offices without locking their computers. Sometimes their screens display sensitive company information. You configure all machines to lock after five minutes of inactivity [a,b]. You also remind your coworkers to lock their systems when they walk away [a].

Potential Assessment Considerations

- Does the session lock hide previously visible information (e.g., replacing what was visible with a lock screen or screensaver that does not include sensitive information) [c]?
- If session locks are not managed centrally, how are all computer users made aware of the requirements and how to configure them [a,b,c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.10

AC.L2-3.1.11 – SESSION TERMINATION

Terminate (automatically) a user session after a defined condition.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] conditions requiring a user session to terminate are defined; and

[b] a user session is automatically terminated after any of the defined conditions occur.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing session termination; system design documentation; system security plan; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing user session termination].

DISCUSSION [NIST SP 800-171 R2]

This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational 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 organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

FURTHER DISCUSSION

Configure the system to terminate user sessions based on the organization's policy. Session termination policies can be simple or sophisticated. Examples are inactivity (end the session

after a specified duration (e.g., one hour[7]) of inactivity), day/time (all sessions are terminated at the end of the established workday), misbehavior (end the session due to an attempted policy violation), and maintenance (terminate sessions to prevent issues with an upgrade or service outage). If there is no automatic control of user sessions, an attacker can take advantage of an unattended session.

Example 1

You are the system administrator for your organization and configure the system to terminate all user sessions after 1 hour of inactivity [a]. As the session timeout approaches, the system prompts users with a warning banner asking if they want to continue the session. When the session timeout does occur, the login page pops up, and the users must log in to start a new session [b].

Example 2

A user is logged into a corporate database containing CUI but is not authorized to view CUI. The user has submitted a series of queries that unintentionally violate policy, as they attempt to extract CUI that the user is not authorized to view [a]. The session terminates with a warning as a result of a violation of corporate policy [b]. The user must reestablish the session before being able to submit additional legitimate queries.

Potential Assessment Considerations

- Are the conditions in which a user session must be terminated described (e.g., after a period of inactivity or after a defined time limit) [a]?
- Are procedures documented that describe how to configure the system to enable automatic termination of user sessions after any of the defined conditions occur [b]?
- Are user sessions terminated based on organizationally defined conditions [a,b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.11

[7] Review DoD Cybersecurity FAQ Q53.2 for information on minimum values.

AC.L2-3.1.12 – CONTROL REMOTE ACCESS

Monitor and control remote access sessions.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] remote access sessions are permitted;

[b] the types of permitted remote access are identified;

[c] remote access sessions are controlled; and

[d] remote access sessions are monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; remote access authorizations; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for managing remote access connections; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Remote access management capability for the system].

DISCUSSION [NIST SP 800-171 R2]

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing

connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

NIST SP 800-46, SP 800-77, and SP 800-113 provide guidance on secure remote access and virtual private networks.

FURTHER DISCUSSION

Remote access connections pass through untrusted networks and therefore require proper security controls such as encryption to ensure data confidentiality. Initialization of all remote sessions should ensure that only authorized users and devices are connecting. After the remote session is established, the connection is monitored to track who is accessing the network remotely and what files are being accessed during the session.

Remote access sessions can encompass more than just remote connections back to a headquarters network. Access to cloud-based email providers or server infrastructures also are relevant to this practice if those environments contain CUI.

This practice, AC.L2-3.1.12, requires the control of remote access sessions and complements five other practices dealing with remote access (AC.L2-3.1.14, AC.L2-3.1.13, AC.L2-3.1.15, IA.L2-3.5.3, and MA.L2-3.7.5):

- AC.L2-3.1.14 limits remote access to specific access control points.
- AC.L2-3.1.13 requires the use of cryptographic mechanisms when enabling remote sessions.
- AC.L2-3.1.15 requires authorization for privileged commands executed during a remote session.
- IA.L2-3.5.3 requires multifactor authentication for network access to non-privileged accounts.
- Finally, MA.L2-3.7.5 requires the addition of multifactor authentication for remote maintenance sessions.

Example

You often need to work from remote locations, such as your home or client sites, and you are permitted to access your organization's internal networks from those remote locations [a]. A system administrator issues you a company laptop with VPN software installed, which is required to connect to the networks remotely [b]. After the laptop connects to the VPN server, you must accept a privacy notice that states that the company's security department may monitor the connection. This monitoring is achieved through the analysis of data from sensors on the network notifying IT if issues arise. The security department may also review audit logs to see who is connecting remotely, when, and what information they are accessing [d]. During session establishment, the message "Verifying Compliance" means software like a Device Health Check (DHC) application is checking the remote device to ensure it meets the established requirements to connect [c].

Potential Assessment Considerations

- Do policies identify when remote access is permitted and what methods must be used [a,b]?
- Are systems configured to permit only approved remote access sessions (e.g., disallow remote access sessions by default) [c]?
- Are automated or manual mechanisms employed for monitoring remote connections? If the monitoring is manual, does it occur at a frequency commensurate with the level of risk [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.12

AC.L2-3.1.13 – REMOTE ACCESS CONFIDENTIALITY

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and

[b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Cryptographic mechanisms protecting remote access sessions].

DISCUSSION [NIST SP 800-171 R2]

Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography.

FURTHER DISCUSSION

A remote access session involves logging into the organization's systems such as its internal network or a cloud service provider from a remote location such as home or an alternate work site. This remote access session must be secured using FIPS-validated cryptography to provide confidentiality and prevent anyone from deciphering session information exchanges.

When CMMC requires cryptography, it is to protect the confidentiality of CUI. FIPS-validated cryptography means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be

separately validated under FIPS 140. Accordingly, FIPS-validated cryptography is required to meet CMMC practices that protect CUI when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access). 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. This practice, AC.L2-3.1.13, requires the use of cryptographic mechanisms when enabling remote sessions and complements five other practices dealing with remote access (AC.L2-3.1.12, AC.L2-3.1.14, AC.L2-3.1.15, IA.L2-3.5.3, and MA.L2-3.7.5):

- AC.L2-3.1.12 requires the control of remote access sessions.
- AC.L2-3.1.14 limits remote access to specific access control points.
- AC.L2-3.1.15 requires authorization for privileged commands executed during a remote session.
- IA.L2-3.5.3 requires multifactor authentication for network access to non-privileged accounts.
- Finally, MA.L2-3.7.5 requires the addition of multifactor authentication for remote maintenance sessions.

Example

As a system administrator you are responsible for implementing a remote network access capability for users who work offsite. In order to provide session confidentiality, you decide to implement a VPN mechanism and select a product that has completed FIPS 140 validation [a,b].

Potential Assessment Considerations

- Are cryptographic mechanisms used for remote access sessions (e.g., Transport Layer Security (TLS) and Internet Protocol Security (IPSec) using FIPS-validated encryption algorithms) defined and implemented [a,b]? Note that simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140.

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.13

AC.L2-3.1.14 – REMOTE ACCESS ROUTING

Route remote access via managed access control points.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] managed access control points are identified and implemented; and

[b] remote access is routed through managed network access control points.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; list of all managed network access control points; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms routing all remote accesses through managed network access control points].

DISCUSSION [NIST SP 800-171 R2]

Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

FURTHER DISCUSSION

The contractor can route all remote access through a limited number of remote access control points to reduce the attack surface and simplify network management. This allows for better monitoring and control of the remote connections.

This practice, AC.L2-3.1.14, limits remote access to specific access control points and complements five other practices dealing with remote access (AC.L2-3.1.12, AC.L2-3.1.13, AC.L2-3.1.15, IA.L2-3.5.3, and MA.L2-3.7.5):

- AC.L2-3.1.12 requires the control of remote access sessions.

- AC.L2-3.1.13 requires the use of cryptographic mechanisms when enabling remote sessions.
- AC.L2-3.1.15 requires authorization for privileged commands executed during a remote session.
- IA.L2-3.5.3 requires multifactor authentication for network access to non-privileged accounts.
- Finally, MA.L2-3.7.5 requires the addition of multifactor authentication for remote maintenance sessions.

Example

You are a system administrator for a company with many locations, and several employees at different locations need to connect to the organization's networks while working remotely. Because each company location has a direct connection to headquarters, you decide to route all remote access through the headquarters location [a]. All remote traffic is routed through a single location to simplify monitoring [b].

Potential Assessment Considerations

- How many managed access control points are implemented [a]?
- Is all remote access routed through the managed access control points [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.14

AC.L2-3.1.15 – PRIVILEGED REMOTE ACCESS

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] privileged commands authorized for remote execution are identified;

[b] security-relevant information authorized to be accessed remotely is identified;

[c] the execution of the identified privileged commands via remote access is authorized; and

[d] access to the identified security-relevant information via remote access is authorized.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing remote access to the system; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing remote access management].

DISCUSSION [NIST SP 800-171 R2]

A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

FURTHER DISCUSSION

Privileged users are not necessarily allowed to perform their job functions from a remote location. Likewise, not all privileged commands may be executed remotely. Allowing remote execution of privileged commands or remote access to security-relevant information should be avoided if possible. If absolutely necessary, the privileged commands authorized for remote execution should be identified and documented. Document which user roles have permissions to remotely execute privileged commands to make changes and to access security relevant information. Documentation must be used to establish security mechanisms that enforce the policy.

This practice, AC.L2-3.1.15, requires authorization for privileged commands executed during a remote session and complements five other practices dealing with remote access (AC.L2-3.1.12, AC.L2-3.1.14, AC.L2-3.1.13, IA.L2-3.5.3, and MA.L2-3.7.5):

- AC.L2-3.1.12 requires the control of remote access sessions.
- AC.L2-3.1.14 limits remote access to specific access control points.
- AC.L2-3.1.13 requires the use of cryptographic mechanisms when enabling remote sessions.
- IA.L2-3.5.3 requires multifactor authentication for network access to non-privileged accounts.
- Finally, MA.L2-3.7.5 requires the addition of multifactor authentication for remote maintenance sessions.

This practice, AC.L2-3.1.15, also extends AC.L1-3.1.2, which limits the types of transactions and functions that authorized users are permitted to execute.

Example

Your company's Access Control Policy permits certain work roles to remotely perform a limited set of privileged commands from company-owned computers [a]. As a system administrator, you implement controls to enforce who can remotely execute a privileged command, which privileged commands they can execute, and who is allowed access to security relevant information such as audit log configuration settings [a,c,d].

Potential Assessment Considerations

- Does system documentation identify system administration or security functions that can be executed remotely [a]?
- Is execution of the identified privileged commands via remote access only authorized for documented operational needs [c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.15

AC.L2-3.1.16 – WIRELESS ACCESS AUTHORIZATION

Authorize wireless access prior to allowing such connections.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] wireless access points are identified; and

[b] wireless access is authorized prior to allowing such connections.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; configuration management plan; procedures addressing wireless access implementation and usage (including restrictions); system security plan; system design documentation; system configuration settings and associated documentation; wireless access authorizations; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for managing wireless access connections; personnel with information security responsibilities].

Test

[SELECT FROM: Wireless access management capability for the system].

DISCUSSION [NIST SP 800-171 R2]

Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols that provide credential protection and mutual authentication.

FURTHER DISCUSSION

Guidelines from management form the basis for the requirements that must be met prior to authorizing a wireless connection. These guidelines may include the following:

- types of devices, such as corporate or privately owned equipment;
- configuration requirements of the devices; and
- authorization requirements before granting such connections.

AC.L2-3.1.16, AC.L2-3.1.17, and AC.L2-3.1.18 are complementary practices in that they all establish requirements to control the connection of mobile devices and wireless devices through the use of authentication, authorization, and encryption mechanisms.

Example

Your company is implementing a wireless network at its headquarters. You work with management to draft a policy about the use of the wireless network. The policy states that only company-approved devices that contain verified security configuration settings are allowed to connect. The policy also includes usage restrictions that must be followed for anyone who wants to use the wireless network. Authorization is required before devices are allowed to connect to the wireless network [b].

Potential Assessment Considerations

- Is an updated list of approved network devices providing wireless access to the system maintained [a]?
- Are network devices providing wireless access configured to require users or devices be authorized prior to permitting a wireless connection [b]?
- Is wireless access to the system authorized and managed [b]?[8]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.16

[8] NIST Handbook 162 Section 3.1.16

AC.L2-3.1.17 – WIRELESS ACCESS PROTECTION

Protect wireless access using authentication and encryption.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] wireless access to the system is protected using authentication; and

[b] wireless access to the system is protected using encryption.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; system design documentation; procedures addressing wireless implementation and usage (including restrictions); system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing wireless access protections to the system].

DISCUSSION [NIST SP 800-171 R2]

Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems.

FURTHER DISCUSSION

Use a combination of authentication and encryption methods to protect the access to wireless networks. Authenticating users to a wireless access point can be achieved in multiple ways. The most common authentication and encryption methods used include:

- WPA2-PSK (WiFi Protected Access-Pre-shared Key) – This method uses a password or passphrase known by the wireless access point and the client (user device). It is common in small companies that have little turnover because the key must be changed each time an employee leaves in order to prevent the terminated employee from connecting to the network without authorization. WPA2 is typically configured to use Advanced Encryption Standard (AES) encryption.

- WPA2 Enterprise – This method may be better for larger companies and enterprise networks because authentication is based on the identity of the individual user or device rather than a shared password or passphrase. It typically requires a Remote Authentication Dial-in User Service (RADIUS) server for authentication and can provide higher security than WPA2-PSK.

Open authentication must not be used because it authenticates any user and lacks security capabilities.

When CMMC requires cryptography, it is to protect the confidentiality of CUI. Federal Information Processing Standard (FIPS)-validated cryptography means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. Accordingly, FIPS-validated cryptography is required to meet CMMC practices that protect CUI when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access). 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.

AC.L2-3.1.16, AC.L2-3.1.17, and AC.L2-3.1.18 are complementary practices in that they all establish requirements to control the connection of mobile devices and wireless devices through the use of authentication, authorization, and encryption mechanisms.

Example 1

You manage the wireless network at a small company and are installing a new wireless solution. You start by selecting a product that employs encryption validated against the FIPS 140 standard. You configure the wireless solution to use WPA2, requiring users to enter a pre-shared key to connect to the wireless network [a,b].

Example 2

You manage the wireless network at a large company and are installing a new wireless solution. You start by selecting a product that employs encryption that is validated against the FIPS 140 standard. Because of the size of your workforce, you configure the wireless system to authenticate users with a RADIUS server. Users must provide the wireless system with their domain usernames and passwords to be able to connect, and the RADIUS server verifies those credentials. Users unable to authenticate are denied access [a,b].

Potential Assessment Considerations

- Is wireless access limited only to authenticated and authorized users (e.g., required to supply a username and password) [a]?
- If the organization is securing its wireless network with a pre-shared key, is access to that key restricted to only authorized users [a]?

- Is wireless access encrypted using FIPS-validated cryptography? Note that simply using an approved algorithm is not sufficient; the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140 [b].[9]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.17

[9] NIST Handbook 162 Section 3.1.17

AC.L2-3.1.18 – MOBILE DEVICE CONNECTION

Control connection of mobile devices.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] mobile devices that process, store, or transmit CUI are identified;

[b] mobile device connections are authorized; and

[c] mobile device connections are monitored and logged.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; authorizations for mobile device connections to organizational systems; procedures addressing access control for mobile device usage (including restrictions); system design documentation; configuration management plan; system security plan; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel using mobile devices to access organizational systems; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Access control capability authorizing mobile device connections to organizational systems].

DISCUSSION [NIST SP 800-171 R2]

A mobile device is a 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 or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches;

conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements. NIST SP 800-124 provides guidance on mobile device security.

FURTHER DISCUSSION

Establish guidelines and acceptable practices for proper configuration, use, and management of mobile devices. Devices that process, store, or transmit CUI must be identified with a device-specific identifier. There are many different types of identifiers, and it is important to select one that can accommodate all devices and be used in a consistent manner. These identifiers are important for facilitating the required monitoring and logging function.

In addition to smartphones, consider the security of other portable devices such as e-readers and tablets.

AC.L2-3.1.16, AC.L2-3.1.17, and AC.L2-3.1.18 are complementary practices in that they all establish requirements to control the connection of mobile devices and wireless devices through the use of authentication, authorization, and encryption mechanisms.

Example

Your organization has a policy stating that all mobile devices, including iPads, tablets, mobile phones, and Personal Digital Assistants (PDAs), must be approved and registered with the IT department before connecting to the network. The IT department uses a Mobile Device Management solution to monitor mobile devices and enforce policies across the enterprise [b,c].

Potential Assessment Considerations

- Is a list of mobile devices that are permitted to process, store, or transmit CUI maintained [a,b]?
- Is the system configured to only permit connections from identified, authorized mobile devices [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.18

AC.L2-3.1.19 – ENCRYPT CUI ON MOBILE

Encrypt CUI on mobile devices and mobile computing platforms.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; and

[b] encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings and associated documentation; encryption mechanisms and associated configuration documentation; system security plan; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with access control responsibilities for mobile devices; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Encryption mechanisms protecting confidentiality of information on mobile devices].

DISCUSSION [NIST SP 800-171 R2]

Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including encrypting selected data structures such as files, records, or fields.

FURTHER DISCUSSION

Ensure CUI is encrypted on all mobile devices and mobile computing platforms that process, store, or transmit CUI including smartphones, tablets, and e-readers.

When CMMC requires cryptography, it is to protect the confidentiality of CUI. FIPS-validated cryptography means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be

separately validated under FIPS 140. Accordingly, FIPS-validated cryptography is required to meet CMMC practices that protect CUI when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access). 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.

This practice, AC.L2-3.1.19, requires that CUI be encrypted on mobile devices and extends three other CUI protection practices (MP.L2-3.8.1, MP.L2-3.8.2, and SC.L2-3.13.16):

- MP.L2-3.8.1 requires that media containing CUI be protected.
- MP.L2-3.8.2 limits access to CUI to authorized users.
- Finally, SC.L2-3.13.16 requires confidentiality of CUI at rest.

This practice, AC.L2-3.1.19, also leverages SC.L2-3.13.11, which specifies that the algorithms used must be FIPS-validated, and SC.L2-3.13.10, which specifies that any cryptographic keys in use must be protected.

Example

You are in charge of mobile device security. You configure all laptops to use the full-disk encryption technology built into the operating system. This approach is FIPS-validated and encrypts all files, folders, and volumes.

Phones and tablets pose a greater technical challenge with their wide range of manufacturers and operating systems. You select a proprietary mobile device management (MDM) solution to enforce FIPS-validated encryption on those devices [a,b].

Potential Assessment Considerations

- Is a list maintained of mobile devices and mobile computing platforms that are permitted to process, store, or transmit CUI [a]?
- Is CUI encrypted on mobile devices using FIPS-validated algorithms [b]?

KEY REFERENCE

- NIST SP 800-171 Rev 2 3.1.19

AC.L2-3.1.21 – PORTABLE STORAGE USE

Limit use of portable storage devices on external systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the use of portable storage devices containing CUI on external systems is identified and documented;

[b] limits on the use of portable storage devices containing CUI on external systems are defined; and

[c] the use of portable storage devices containing CUI on external systems is limited as defined.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing the use of external systems; system security plan; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for restricting or prohibiting use of organization-controlled storage devices on external systems; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing restrictions on use of portable storage devices].

DISCUSSION [NIST SP 800-171 R2]

Limits on the use of organization-controlled portable storage devices in external systems include 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. Note that while “external” typically refers to outside of the organization’s direct supervision and authority that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.

FURTHER DISCUSSION

A portable storage device is a system component that can be inserted or attached and easily removed from a system. It is used to store data or information. Examples of portable storage devices include:

- compact/digital video disks (CDs/DVDs);
- Universal Serial Bus (USB) drives;
- external hard disk drives;
- flash memory cards/drives; and
- floppy disks.

This practice can be implemented in two ways:

- identifying the portable storage device usage restrictions, identifying portable storage devices that may be used on external systems, identifying associated external systems on which a portable storage device may be used, and administratively (through the use of a written policy) limiting the usage of the devices to those systems; or
- configuring devices to work only when connected to a system to which the portable storage device can authenticate, limiting the devices' use on external systems to those that the contractor has the ability to manage.

Example

Your organization has a written portable device usage restriction policy. It states that users can only use external storage devices such as thumb dives or external hard disks that belong to the company. When needed for a specific business function, a user checks the device out from IT and returns it to IT when no longer needed [a,b].

Potential Assessment Considerations

- Are the portable storage devices authorized for external use identified and documented [a]?
- Are the circumstances defined in which portable storage devices containing CUI may be used on external systems (e.g., with management approval) [b]?
- Are limitations stipulated for the use of portable storage devices containing CUI on external systems (e.g., authorized personnel only, encrypted drives required) [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.1.21

Awareness and Training (AT)

Level 2 AT Practices

AT.L2-3.2.1 – ROLE-BASED RISK AWARENESS

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] security risks associated with organizational activities involving CUI are identified;

[b] policies, standards, and procedures related to the security of the system are identified;

[c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities; and

[d] managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training].

Test

[SELECT FROM: Mechanisms managing security awareness training; mechanisms managing role-based security training].

DISCUSSION [NIST SP 800-171 R2]

Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel 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 include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

NIST SP 800-50 provides guidance on security awareness and training programs.

FURTHER DISCUSSION

Awareness training focuses user attention on security. Several techniques can be used, such as:

- synchronous or asynchronous training;
- simulations (e.g., simulated phishing emails);
- security awareness campaigns (posters, reminders, group discussions); and
- communicating regular email advisories and notices to employees.

Awareness training and role-based training are different. This practice, AT.L2-3.2.1, covers awareness training, which provides general security training to influence user behavior. This training can apply broadly or be tailored to a specific role. Role-based training focuses on the knowledge, skills, and abilities needed to complete a specific job and is covered by AT.L2-3.2.2.

Example

You want to provide information to employees so they can identify phishing emails. To do this, you prepare a presentation that highlights basic traits, including:

- suspicious-looking email address or domain name;
- a message that contains an attachment or URL; and
- a message that is poorly written and often contains obvious misspelled words.

You encourage everyone to not click on attachments or links in a suspicious email [c]. You tell employees to forward such a message immediately to IT security [d]. You download free security awareness posters to hang in the office [c,d]. You send regular emails and tips to all employees to ensure your message is not forgotten over time [c,d].

Potential Assessment Considerations

- Do all users, managers, and system administrators receive initial and refresher training commensurate with their roles and responsibilities [c,d]?[10]

[10] NIST Handbook 162 Section 3.2.1

- Do training materials identify the organizationally defined security requirements that must be met by users while interacting with the system as described in written policies, standards, and procedures [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.2.1

AT.L2-3.2.2 – ROLE-BASED TRAINING

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] information security-related duties, roles, and responsibilities are defined;

[b] information security-related duties, roles, and responsibilities are assigned to designated personnel; and

[c] personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel representing the general system user community].

Test

[SELECT FROM: Mechanisms managing role-based security training; mechanisms managing security awareness training].

DISCUSSION [NIST SP 800-171 R2]

Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, 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 controls. Such training can include policies, procedures, tools, and artifacts for the 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 organizational information security programs.

NIST SP 800-181 provides guidance on role-based information security training in the workplace. SP 800-161 provides guidance on supply chain risk management.

FURTHER DISCUSSION

Training imparts skills and knowledge to enable staff to perform a specific job function. Training should be available to all employees for all organizational roles to accommodate role changes without being constrained by the training schedule. Awareness training and role-based training are different. Awareness training provides general security training to influence user behavior and is covered by AT.L2-3.2.1. This practice, AT.L2-3.2.2, covers role-based training that focuses on the knowledge, skills, and abilities needed to complete a specific job. Role-based training may include awareness topics specific to individual roles such as ensuring systems administrators understand the risk associated with using an administrative account.

Example

Your company upgraded the firewall to a newer, more advanced system. You have been identified as an employee who needs training on the new device [a,b,c]. This will enable you to use the firewall effectively and efficiently. Your company considered training resources when it planned for the upgrade and ensured that training funds were available as part of the upgrade project [c].

Potential Assessment Considerations

- Are the duties, roles, and responsibilities that impact, directly or indirectly, the information security of the company or its systems defined and documented [a]?
- Do information security-related tasks have accountable owners, and is a strictly limited group of individuals assigned to perform them [b]?
- Are personnel who are assigned information security-related duties, roles, and responsibilities trained on those responsibilities, including the security requirements unique or inherent to their roles or responsibilities [c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.2.2

AT.L2-3.2.3 – INSIDER THREAT AWARENESS

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] potential indicators associated with insider threats are identified; and

[b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; insider threat policy and procedures; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel that participate in security awareness training; personnel with responsibilities for basic security awareness training; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms managing insider threat training].

DISCUSSION [NIST SP 800-171 R2]

Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

FURTHER DISCUSSION

An insider threat is the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm. Insider threat security awareness training focuses on recognizing employee behaviors and characteristics that might be indicators of an insider threat and the guidelines and procedures to handle and report it. Training for managers will provide guidance on observing team members to identify all potential threat indicators, while training for general employees will provide guidance for focusing on a smaller number of indicators. Employee behaviors will vary depending on roles, team membership, and associated information needs. The person responsible for specifying insider threat indicators must be cognizant of these factors. Because of this, organizations may choose to tailor the training for specific roles. This practice does not require separate training regarding insider threat. Organizations may choose to integrate these topics into their standard security awareness training programs.

Example

You are responsible for training all employees on the awareness of high-risk behaviors that can indicate a potential insider threat [b]. You educate yourself on the latest research on insider threat indicators by reviewing a number of law enforcement bulletins [a]. You then add the following example to the training package: A baseline of normal behavior for work schedules has been created. One employee's normal work schedule is 8:00 AM–5:00 PM, but another employee noticed that the employee has been working until 9:00 PM every day even though no projects requiring additional hours have been assigned [b]. The observing employee reports the abnormal work schedule using the established reporting guidelines.

Potential Assessment Considerations

- Do training materials include potential indicators associated with insider threats (e.g., repeated security violations, unusual work hours, unexpected significant transfers of data, suspicious contacts, concerning behaviors outside the workplace) [a,b]?
- Do training materials include methods of reporting potential indicators of insider threats to management or responsible security personnel [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.2.3

Audit and Accountability (AU)

Level 2 AU Practices

AU.L2-3.3.1 – SYSTEM AUDITING

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified;

[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined;

[c] audit records are created (generated);

[d] audit records, once created, contain the defined content;

[e] retention requirements for audit records are defined; and

[f] audit records are retained as defined.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms implementing system audit logging].

DISCUSSION [NIST SP 800-171 R2]

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or failure indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).

Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making. NIST SP 800-92 provides guidance on security log management.

FURTHER DISCUSSION

Contractors must ensure that all applicable systems create and retain audit logs that contain enough information to identify and investigate potentially unlawful or unauthorized system activity. Contractors must define the audit logs it needs to collect as well as the specific events to capture within the selected logs. Captured audit records are checked to verify that they contain the required events.

In defining the audit log retention period, contractors must ensure that logs are retained for a sufficiently long period to allow for the investigation of a security event. The retention

period must take into account the delay of weeks or months that can occur between an initial compromise and the discovery of attacker activity.

Example

You set up audit logging capability for your company. You determine that all systems that contain CUI must have extra detail in the audit logs. Because of this, you configure these systems to log the following information for all user actions [b,c]:

- time stamps;
- source and destination addresses;
- user or process identifiers;
- event descriptions;
- success or fail indications; and
- filenames.

Potential Assessment Considerations

- Are audit log retention requirements appropriate to the system and its associated level of risk [e]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.1

AU.L2-3.3.2 – USER ACCOUNTABILITY

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and

[b] audit records, once created, contain the defined content.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing audit records and event types; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing audit record generation; procedures addressing audit review, analysis, and reporting; reports of audit findings; system audit logs and records; system events; system incident reports; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing system audit logging].

DISCUSSION [NIST SP 800-171 R2]

This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of VoIP.

FURTHER DISCUSSION

Capturing the necessary information in audit logs ensures that you can trace actions to a specific user. This may include capturing user IDs, source and destination addresses, and

time stamps. Logging from networks, servers, clients, and applications should be considered in ensuring accountability.

This practice, AU.L2-3.3.2, which ensures logging and traceability of user actions, supports the control of non-privileged users required by AC.L2-3.1.7 as well as many other auditing, configuration management, incident response, and situation awareness practices.

Example

You are a system administrator. You want to ensure that you can trace all remote access sessions to a specific user. You configure the VPN device to capture the following information for all remote access connections: source and destination IP address, user ID, machine name, time stamp, and user actions during the remote session [b].

Potential Assessment Considerations

- Are users uniquely traced and held responsible for unauthorized actions [a]?
- Does the system protect against an individual denying having performed an action (non-repudiation) [b]?[11]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.2

[11] NIST Handbook 162 3.3.2

AU.L2-3.3.3 – EVENT REVIEW

Review and update logged events.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a process for determining when to review logged events is defined;

[b] event types being logged are reviewed in accordance with the defined review process; and

[c] event types being logged are updated based on the review.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing audit records and event types; system security plan; list of organization-defined event types to be logged; reviewed and updated records of logged event types; system audit logs and records; system incident reports; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting review and update of logged event types].

DISCUSSION [NIST SP 800-171 R2]

The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

FURTHER DISCUSSION

This practice is focused on the configuration of the auditing system, not the review of the audit records produced by the selected events. The review of the audit logs is covered under AU.L2-3.3.5 and AU.L2-3.3.6.

Example

You are in charge of IT operations for your company and are responsible for identifying and documenting which events are relevant to the security of your company's systems. Your

company has decided that this list of events should be updated annually or when new security threats or events have been identified, which may require additional events to be logged and reviewed [a]. The list of events you are capturing in your logs started as the list of recommended events given by the manufacturers of your operating systems and devices, but it has grown from experience.

Your company experiences a security incident, and a forensics review shows the logs appear to have been deleted by a remote user. You notice that remote sessions are not currently being logged [b]. You update the list of events to include logging all VPN sessions [c].

Potential Assessment Considerations

- Do documented processes include methods for determining when to review logged event types (i.e., regular frequency, after incidents, after major system changes) [a]?
- Do documented processes include methods for reviewing event types being logged (i.e., based on specific threat, use case, retention capacity, current utilization, and/or newly added system component or functionality) [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.3

AU.L2-3.3.4 – AUDIT FAILURE ALERTING

Alert in the event of an audit logging process failure.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] personnel or roles to be alerted in the event of an audit logging process failure are identified;

[b] types of audit logging process failures for which alert will be generated are defined; and

[c] identified personnel or roles are alerted in the event of an audit logging process failure.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing response to audit logging processing failures; system design documentation; system security plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit logging processing failure; system incident reports; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing system response to audit logging process failures].

DISCUSSION [NIST SP 800-171 R2]

Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

FURTHER DISCUSSION

Audit logging keeps track of activities occurring on the network, servers, user workstations, and other components of the overall system. These logs must always be available and functional. The company's designated security personnel (e.g., system administrator and

security officer) need to be aware when the audit log process fails or becomes unavailable [a]. Notifications (e.g., email, Short Message Service (SMS)) should to be sent to the company's designated security personnel to immediately take appropriate action. If security personnel are unaware of the audit logging process failure, then they will be unaware of any suspicious activity occurring at that time. Response to an audit logging process failure should account for the extent of the failure (e.g., a single component's audit logging versus failure of the centralized logging solution), the risks involved in this loss of audit logging, and other factors (e.g., the possibility that an adversary could have caused the audit logging process failure).

Example

You are in charge of IT operations for your company, and your responsibilities include managing the audit logging process. You configure your systems to send you an email in the event of an audit log failure. One day, you receive one of these alerts. You connect to the system, restart logging, and determine why the logging stopped [a,b,c].

Potential Assessment Considerations

- Will the system alert personnel with security responsibilities in the event of an audit processing failure?[12]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.4

[12] NIST Handbook 162 Section 3.3.4

AU.L2-3.3.5 – AUDIT CORRELATION

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined; and

[b] defined audit record review, analysis, and reporting processes are correlated.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing audit record review, analysis, and reporting; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing investigation of and response to suspicious activities; system audit logs and records across different repositories; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit record review, analysis, and reporting responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting analysis and correlation of audit records; mechanisms integrating audit review, analysis and reporting].

DISCUSSION [NIST SP 800-171 R2]

Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

FURTHER DISCUSSION

Companies must review, analyze, and report audit records to help detect and respond to security incidents in a timely manner for the purpose of investigation and corrective actions. Collection of audit logs into one or more central repositories may facilitate correlated review. Small companies may be able to accomplish this manually with well-defined and -managed procedures. Larger companies will use an automated system for analysis that correlates log data from across the entire enterprise. Some companies may want to orchestrate the analysis

process to include the use of Application Programming Interfaces (APIs) for collection, correlation, and the automation of responses based on programed rulesets.

Example

You are a member of a cyber defense team responsible for audit log analysis. You run an automated tool that analyzes all the audit logs across a Local Area Network (LAN) segment simultaneously looking for similar anomalies on separate systems at separate locations. After extracting anomalous information and performing a correlation analysis [b], you determine that four different systems have had their event log information cleared between 2:00 AM to 3:00 AM, although the associated dates are different. The team monitors all systems on the same LAN segment between 2:00 AM to 3:00 AM for the next 30 days.

Potential Assessment Considerations

- Are mechanisms used across different repositories to integrate audit review, analysis, correlation, and reporting processes [b]?[13]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.5

[13] NIST Handbook 162 Section 3.3.5

AU.L2-3.3.6 – REDUCTION & REPORTING

Provide audit record reduction and report generation to support on-demand analysis and reporting.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] an audit record reduction capability that supports on-demand analysis is provided; and

[b] a report generation capability that supports on-demand reporting is provided.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing audit record reduction and report generation; system design documentation; system security plan; system configuration settings and associated documentation; audit record reduction, review, analysis, and reporting tools; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit record reduction and report generation responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Audit record reduction and report generation capability].

DISCUSSION [NIST SP 800-171 R2]

Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record 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 system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

FURTHER DISCUSSION

Raw audit log data is difficult to review, analyze, and report because of the volume of data. Audit record reduction is an automated process that interprets raw audit log data and extracts meaningful and relevant information without altering the original logs. An example

of log reduction for files to be analyzed would be the removal of details associated with nightly backups. Report generation on reduced log information allows you to create succinct customized reports without the need to burden the reader with unimportant information. In addition, the security-relevant audit information must be made available to personnel on demand for immediate review, analysis, reporting, and event investigation support. Performing audit log reduction and providing on-demand reports may allow the analyst to take mitigating action before an adversary completes its malicious actions.

Example

You are in charge of IT operations in your company. You are responsible for providing audit record reduction and report generation capability. To support this function, you deploy an open-source solution that will collect and analyze data for signs of anomalies. The solution queries your central log repository to extract relevant data and provide you with a concise and comprehensive view for further analysis to identify potentially malicious activity [a]. In addition to creating on-demand data sets for analysis, you create customized reports explaining the contents of the data set [b].

Potential Assessment Considerations

- Does the system support on-demand audit review, analysis, and reporting requirements and after-the-fact security investigations [b]?[14]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.6

[14] NIST Handbook 162 Section 3.3.6

AU.L2-3.3.7 – AUTHORITATIVE TIME SOURCE

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] internal system clocks are used to generate time stamps for audit records;

[b] an authoritative source with which to compare and synchronize internal system clocks is specified; and

[c] internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Mechanisms implementing time stamp generation; mechanisms implementing internal information system clock synchronization].

DISCUSSION [NIST SP 800-171 R2]

Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

FURTHER DISCUSSION

Each system must synchronize its time with a central time server to ensure that all systems are recording audit logs using the same time source. Reviewing audit logs from multiple systems can be a difficult task if time is not synchronized. Systems can be synchronized to a network device or directory service or configured manually.

Example

You are setting up several new computers on your company's network. You update the time settings on each machine to use the same authoritative time server on the internet [b,c]. When you review audit logs, all your machines will have synchronized time, which aids in any potential security investigations.

Potential Assessment Considerations

- Can the records' time stamps map to Coordinated Universal Time (UTC), compare system clocks with authoritative Network Time Protocol (NTP) servers, and synchronize system clocks when the time difference is greater than 1 second [c]?[15]
- Does the system synchronize internal system clocks on a defined frequency [c]?[16]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.7

[15] NIST Handbook 162 Section 3.3.7
[16] NIST Handbook 162 Section 3.3.7

AU.L2-3.3.8 – AUDIT PROTECTION

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] audit information is protected from unauthorized access;

[b] audit information is protected from unauthorized modification;

[c] audit information is protected from unauthorized deletion;

[d] audit logging tools are protected from unauthorized access;

[e] audit logging tools are protected from unauthorized modification; and

[f] audit logging tools are protected from unauthorized deletion.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation, system audit logs and records; audit logging tools; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing audit information protection].

DISCUSSION [NIST SP 800-171 R2]

Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.

FURTHER DISCUSSION

Audit information is a critical record of what events occurred, the source of the events, and the outcomes of the events; this information needs to be protected. The logs must be properly secured so that the information may not be modified or deleted, either intentionally or unintentionally. Only those with a legitimate need-to-know should have access to audit information, whether that information is being accessed directly from logs or from audit tools.

Example

You are in charge of IT operations in your company. Your responsibilities include protecting audit information and audit logging tools. You protect the information from modification or deletion by having audit log events forwarded to a central server and by restricting the local audit logs to only be viewable by the system administrators [a,b,c]. Only a small group of security professionals can view the data on the central audit server [b,c,d]. For an additional layer of protection, you back up the server daily and encrypt the backups before sending them to a cloud data repository [a,b,c].

Potential Assessment Considerations

- Is there a list of authorized users for audit systems and tools [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.8

AU.L2-3.3.9 – AUDIT MANAGEMENT

Limit management of audit logging functionality to a subset of privileged users.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a subset of privileged users granted access to manage audit logging functionality is defined; and

[b] management of audit logging functionality is limited to the defined subset of privileged users.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

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

Interview

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

Test

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

DISCUSSION [NIST SP 800-171 R2]

Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

FURTHER DISCUSSION

Companies should restrict access to audit logging functions to a limited number of privileged users who can modify audit logs and audit settings. General users should not be granted permissions to perform audit management. All audit managers should be privileged users, but only a small subset of privileged users will be given audit management responsibilities.

Functions performed by privileged users must be distinctly separate from the functions performed by users who have audit-related responsibilities to reduce the potential of fraudulent activities by privileged users not being detected or reported. When possible, individuals who manage audit logs should not have access to other privileged functions.

Example

You are a junior system administrator responsible for the administration of select company infrastructure, but you are not responsible for managing audit information. You are not permitted to review audit logs, delete audit logs, or modify audit log settings [b]. Full control of audit logging functions has been given to senior system administrators [a,b]. This separation of system administration duties from audit logging management is necessary to prevent possible log file tampering.

Potential Assessment Considerations

- Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected [b]?[17]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.3.9

[17] NIST Handbook 162 Section 3.3.9

Configuration Management (CM)

Level 2 CM Practices

CM.L2-3.4.1 – SYSTEM BASELINING

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a baseline configuration is established;

[b] the baseline configuration includes hardware, software, firmware, and documentation;

[c] the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle;

[d] a system inventory is established;

[e] the system inventory includes hardware, software, firmware, and documentation; and

[f] the inventory is maintained (reviewed and updated) throughout the system development life cycle.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; procedures addressing system inventory; system security plan; configuration management plan; system inventory records; inventory review and update records; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system component installation records; system component removal records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organizational processes for updating inventory of system components; mechanisms supporting or implementing the system inventory; mechanisms implementing updating of the system inventory].

DISCUSSION [NIST SP 800-171 R2]

This requirement establishes and maintains baseline configurations for systems and system components including for system communications and connectivity. Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration.

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include manufacturer, device type, model, serial number, and physical location.

NIST SP 800-128 provides guidance on security-focused configuration management.

FURTHER DISCUSSION

An effective cybersecurity program depends on consistent, secure system and component configuration and management. Build and configure systems from a known, secure, and approved configuration baseline. This includes:

- documenting the software and configuration settings of a system;
- placement within the network; and
- other specifications as required by the organization.

Example

You are in charge of upgrading the computer operating systems of your office's computers. You research how to set up and configure a workstation with the least functionality and highest security and use that as the framework for creating a configuration that minimizes functionality while still allowing users to do their tasks. After testing the new baseline on a single workstation, you document this configuration and apply it to the other computers [a]. You then check to make sure that the software changes are accurately reflected in your master system inventory [e]. Finally, you set a calendar reminder to review the baseline in three months [f].

Potential Assessment Considerations

- Do baseline configurations include software versions and patch level, configuration parameters, network information, and communications with connected systems [a,b]?[18]
- Are baseline configurations updated as needed to accommodate security risks or software changes [c]?[19]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.1

[18] NIST Handbook 162 Section 3.4.1
[19] NIST Handbook 162 Section 3.4.1

CM.L2-3.4.2 – SECURITY CONFIGURATION ENFORCEMENT

Establish and enforce security configuration settings for information technology products employed in organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] security configuration settings for information technology products employed in the system are established and included in the baseline configuration; and

[b] security configuration settings for information technology products employed in the system are enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; baseline configuration; procedures addressing configuration settings for the system; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; evidence supporting approved deviations from established configuration settings; change control records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings; processes for managing baseline configurations; mechanisms supporting configuration control of baseline configurations].

DISCUSSION [NIST SP 800-171 R2]

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

NIST SP 800-70 and SP 800-128 provide guidance on security configuration settings.

FURTHER DISCUSSION

Information security is an integral part of a company's configuration management process. Security-related configuration settings are customized to satisfy the company's security requirements and are applied them to all systems once tested and approved. The configuration settings must reflect the most restrictive settings that are appropriate for the system. Any required deviations from the baseline are reviewed, documented, and approved.

Example

You manage baseline configurations for your company's systems. As part of this, you download a secure configuration guide for each of your asset types (servers, workstations, network components, operating systems, middleware, and applications) from a well-known and trusted IT security organization. You then apply all of the settings that you can while still ensuring the assets can perform the role for which they are needed. Once you have the configuration settings identified and tested, you document them to ensure all applicable machines can be configured the same way [a,b].

Potential Assessment Considerations

- Do security settings reflect the most restrictive settings appropriate [a]?[20]
- Are changes or deviations to security settings documented [b]?[21]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.2

[20] NIST Handbook 162 Section 3.4.2
[21] NIST Handbook 162 Section 3.4.2

CM.L2-3.4.3 – SYSTEM CHANGE MANAGEMENT

Track, review, approve or disapprove, and log changes to organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] changes to the system are tracked;

[b] changes to the system are reviewed;

[c] changes to the system are approved or disapproved; and

[d] changes to the system are logged.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; system security plan; change control records; system audit logs and records; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; other relevant documents or records].

Interview

[SELECT FROM: Personnel with configuration change control responsibilities; personnel with information security responsibilities; system or network administrators; members of change control board or similar].

Test

[SELECT FROM: Organizational processes for configuration change control; mechanisms that implement configuration change control].

DISCUSSION [NIST SP 800-171 R2]

Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems.

For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.

NIST SP 800-128 provides guidance on configuration change control.

FURTHER DISCUSSION

You must track, review, and approve configuration changes before committing to production. Changes to computing environments can create unintended and unforeseen issues that can affect the security and availability of the systems. Relevant experts and stakeholders must review and approve proposed changes. They should discuss potential impacts before the organization puts the changes in place. Relevant items include changes to the physical environment and to the systems hosted within it.

Example

Once a month, the management and technical team leads join a change control board meeting. During this meeting, everyone reviews all proposed changes to the environment [b,c]. This includes changes to the physical and computing environments. The meeting ensures that relevant subject-matter experts review changes and propose alternatives where needed.

Potential Assessment Considerations

- Are changes to the system authorized by company management and documented [a,b,c,d]?[22]
- Are changes documented and tracked (e.g., manually written down or included in a tracking service such as a ticketing system) [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.3

[22] NIST Handbook 162 Section 3.4.3

CM.L2-3.4.4 – SECURITY IMPACT ANALYSIS

Analyze the security impact of changes prior to implementation.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the security impact of changes to the system is analyzed prior to implementation.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing security impact analysis for system changes; configuration management plan; security impact analysis documentation; system security plan; analysis tools and associated outputs; change control records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibility for conducting security impact analysis; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for security impact analysis].

DISCUSSION [NIST SP 800-171 R2]

Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

NIST SP 800-128 provides guidance on configuration change control and security impact analysis.

FURTHER DISCUSSION

Changes to complex environments are reviewed for potential security impact before implemented. Changes to IT systems can cause unforeseen problems and have unintended consequences for both users and the security of the operating environment. Analyze the

security impact of changes prior to implementing them. This can uncover and mitigate potential problems before they occur.

Example

You have been asked to deploy a new web browser plug-in. Your standard change management process requires that you produce a detailed plan for the change, including a review of its potential security impact. A subject-matter expert who did not submit the change reviews the plan and tests the new plug-in for functionality and security. You update the change plan based on the expert's findings and submit it to the change control board for final approval [a].

Potential Assessment Considerations

- Are configuration changes tested, validated, and documented before installing them on the operational system [a]?[23]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.4

[23] NIST Handbook 162 Section 3.4.4

CM.L2-3.4.5 – ACCESS RESTRICTIONS FOR CHANGE

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] physical access restrictions associated with changes to the system are defined;

[b] physical access restrictions associated with changes to the system are documented;

[c] physical access restrictions associated with changes to the system are approved;

[d] physical access restrictions associated with changes to the system are enforced;

[e] logical access restrictions associated with changes to the system are defined;

[f] logical access restrictions associated with changes to the system are documented;

[g] logical access restrictions associated with changes to the system are approved; and

[h] logical access restrictions associated with changes to the system are enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; system security plan; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with logical access control responsibilities; personnel with physical access control responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for managing access restrictions associated with changes to the system; mechanisms supporting, implementing, and enforcing access restrictions associated with changes to the system].

DISCUSSION [NIST SP 800-171 R2]

Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating

changes, including upgrades and modifications. Access restrictions for change also include software libraries. Access restrictions include physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during certain specified times). In addition to security concerns, commonly-accepted due diligence for configuration management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration.

NIST SP 800-128 provides guidance on configuration change control.

FURTHER DISCUSSION

Define, identify, and document qualified individuals authorized to make physical and logical changes to the organization's hardware, software, software libraries, or firmware components. Control of configuration management activities may involve:

- physical access control that prohibits unauthorized users from gaining physical access to an asset (e.g., requiring a special key card to enter a server room);
- logical access control that prevents unauthorized users from logging onto a system to make configuration changes (e.g., requiring specific credentials for modifying configuration settings, patching software, or updating software libraries);
- workflow automation in which configuration management workflow rules define human tasks and data or files are routed between people authorized to do configuration management based on pre-defined business rules (e.g., passing an electronic form to a manager requesting approval of configuration change made by an authorized employee);
- an abstraction layer for configuration management that requires changes be made from an external system through constrained interface (e.g., software updates can only be made from a patch management system with a specific IP address); and
- utilization of a configuration management change window (e.g., software updates are only allowed between 8:00 AM and 10:00 AM or between 6:00 PM and 8:00 PM).

Example

Your datacenter requires expanded storage capacity in a server. The change has been approved, and security is planning to allow an external technician to access the building at a specific date and time under the supervision of a manager [a,b,c,d]. A system administrator creates a temporary privileged account that can be used to log into the server's operating system and update storage settings [e,f,g]. On the appointed day, the technician is escorted into the datacenter, upgrades the hardware, expands the storage in the operating system (OS), and departs. The manager verifies the upgrade and disables the privileged account [h].

Potential Assessment Considerations

- Are only employees who are approved to make physical or logical changes on systems allowed to do so [a,d,e,h]?[24]
- Are authorized personnel approved and documented by the service owner and IT security [a,e]?[25]
- Does all change documentation include the name of the authorized employee making the change [b,d,f,h]?[26]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.5

[24] NIST Handbook 162 Section 3.4.5
[25] NIST Handbook 162 Section 3.4.5
[26] NIST Handbook 162 Section 3.4.5

CM.L2-3.4.6 – LEAST FUNCTIONALITY

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] essential system capabilities are defined based on the principle of least functionality; and

[b] the system is configured to provide only the defined essential capabilities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; configuration management plan; procedures addressing least functionality in the system; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes prohibiting or restricting functions, ports, protocols, or services; mechanisms implementing restrictions or prohibition of functions, ports, protocols, or services].

DISCUSSION [NIST SP 800-171 R2]

Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components. However, doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component.

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations 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.

FURTHER DISCUSSION

You should customize organizational systems to remove non-essential applications and disable unnecessary services. Systems come with many unnecessary applications and settings enabled by default including unused ports and protocols. Leave only the fewest capabilities necessary for the systems to operate effectively.

Example

You have ordered a new server, which has arrived with a number of free utilities installed in addition to the operating system. Before you deploy the server, you research the utilities to determine which ones can be eliminated without impacting functionality. You remove the unneeded software, then move on to disable unused ports and services. The server that enters production therefore has only the essential capabilities enabled for the system to function in its role [a,b].

Potential Assessment Considerations

- Are the roles and functions for each system identified along with the software and services required to perform those functions [a]?
- Are the software and services required for those defined functions identified [a]?
- Is the information system configured to exclude any function not needed in the operational environment [b]?[27]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.6

[27] NIST Handbook 162 Section 3.4.6

CM.L2-3.4.7 – NONESSENTIAL FUNCTIONALITY

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] essential programs are defined;

[b] the use of nonessential programs is defined;

[c] the use of nonessential programs is restricted, disabled, or prevented as defined;

[d] essential functions are defined;

[e] the use of nonessential functions is defined;

[f] the use of nonessential functions is restricted, disabled, or prevented as defined;

[g] essential ports are defined;

[h] the use of nonessential ports is defined;

[i] the use of nonessential ports is restricted, disabled, or prevented as defined;

[j] essential protocols are defined;

[k] the use of nonessential protocols is defined;

[l] the use of nonessential protocols is restricted, disabled, or prevented as defined;

[m] essential services are defined;

[n] the use of nonessential services is defined; and

[o] the use of nonessential services is restricted, disabled, or prevented as defined.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system security plan; system design documentation; security configuration checklists; system configuration settings and associated documentation; specifications for preventing software program execution; documented reviews of programs, functions, ports, protocols, and/or services; change control records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for reviewing programs, functions, ports, protocols, and services on the system; personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services; mechanisms implementing review and handling of nonessential programs, functions, ports, protocols, or services; organizational processes preventing program execution on the system; organizational processes for software program usage and restrictions; mechanisms supporting or implementing software program usage and restrictions; mechanisms preventing program execution on the system].

DISCUSSION [NIST SP 800-171 R2]

Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.

FURTHER DISCUSSION

Organizations should only use the minimum set of programs, services, ports, and protocols required for to accomplish the organization's mission. This has several implications:

- All unnecessary programs and accounts are removed from all endpoints and servers.
- The organization makes a policy decision to control the execution of programs through either whitelisting or blacklisting. Whitelisting means a program can only run if the software has been vetted in some way, and the executable name has been entered onto a list of allowed software. Blacklisting means any software can execute as long it is not on a list of known malicious software. Whitelisting provides far more security than blacklisting, but the organization's policy can direct the implementation of either approach. Control of execution applies to both servers and endpoints.
- The organization restricts the use of all unnecessary ports, protocols, and system services in order to limit entry points that attackers can use. For example, the use of the FTP service is eliminated from all computers, and the associated ports are blocked unless a required service utilizes those ports. The elimination of nonessential functionality on the network and systems provides a smaller attack surface for an attacker to gain access and take control of your network or systems.

This practice, CM.L2-3.4.7, which requires limiting functionality to essential programs, ports, protocols, and services, extends CM.L2-3.4.6, which requires adherence to the principle of least functionality but does not specifically address which elements of a system should be limited.

Example

You are responsible for purchasing new endpoint hardware, installing organizationally required software to the hardware, and configuring the endpoint in accordance with the

organization's policy. The organization has a system imaging capability that loads all necessary software, but it does not remove unnecessary services, eliminate the use of certain protocols, or close unused ports. After imaging the systems, you close all ports and block the use of all protocols except the following:

- TCP for SSH on port 22;
- SMTP on port 25;
- TCP and UDP on port 53; and
- HTTP and HTTPS on port 443.

The use of any other ports or protocols are allowed by exception only [i,l,o].

Potential Assessment Considerations

- Are only applications and services that are needed for the function of the system configured and enabled [a,b,c,d,e,f]?[28]
- Are only those ports and protocols necessary to provide the service of the information system configured for that system [g,h,i,j,k,l]?[29]
- Are systems services reviewed to determine what is essential for the function of that system [m]?[30]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.7

[28] NIST Handbook 162 Section 3.4.7
[29] NIST Handbook 162 Section 3.4.7
[30] NIST Handbook 162 Section 3.4.7

CM.L2-3.4.8 – APPLICATION EXECUTION POLICY

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a policy specifying whether whitelisting or blacklisting is to be implemented is specified;

[b] the software allowed to execute under whitelisting or denied use under blacklisting is specified; and

[c] whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; system security plan; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs not authorized to execute on the system; list of software programs authorized to execute on the system; security configuration checklists; review and update records associated with list of authorized or unauthorized software programs; change control records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for identifying software authorized or not authorized to execute on the system; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational process for identifying, reviewing, and updating programs authorized or not authorized to execute on the system; process for implementing blacklisting or whitelisting; mechanisms supporting or implementing blacklisting or whitelisting].

DISCUSSION [NIST SP 800-171 R2]

The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution.

In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

NIST SP 800-167 provides guidance on application whitelisting.

FURTHER DISCUSSION

Organizations should determine their blacklisting or whitelisting policy and configure the system to manage software that is allowed to run. Blacklisting or deny-by-exception allows all software to run except if on an unauthorized software list such as what is maintained in antivirus solutions. Whitelisting or permit-by-exception does not allow any software to run except if on an authorized software list. The stronger policy of the two is whitelisting.

This practice, CM.L2-3.4.8, requires the implementation of allow-lists and deny-lists for application software. It leverages CM.L2-3.4.1, which requires the organization to establish and maintain software inventories.

This practice, CM.L2-3.4.8, also extends CM.L2-3.4.9, which only requires control and monitoring of any user installed software.

Example

To improve your company's protection from malware, you have decided to allow only designated programs to run. With additional research you identify a capability within the latest operating system that can control executables, scripts, libraries, or application installers run in your environment [c]. To ensure success you begin by authorizing digitally signed executables. Once they are deployed, you then plan to evaluate and deploy whitelisting for software libraries and scripts [c].

Potential Assessment Considerations

- Is the information system configured to only allow authorized software to run [a,b,c]?[31]
- Is the system configured to disallow running unauthorized software [a,b,c]?[32]
- Is there a defined list of software programs authorized to execute on the system [b]?[33]
- Is the authorization policy a deny-all, permit by exception for software allowed to execute on the system [a,b,c]?[34]
- Are automated mechanisms used to prevent program execution in accordance with defined lists (e.g., white listing) [a,b,c]?[35]

[31] NIST Handbook 162 Section 3.4.8
[32] NIST Handbook 162 Section 3.4.8
[33] NIST Handbook 162 Section 3.4.8
[34] NIST Handbook 162 Section 3.4.8
[35] NIST Handbook 162 Section 3.4.8

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.8

CM.L2-3.4.9 – USER-INSTALLED SOFTWARE

Control and monitor user-installed software.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a policy for controlling the installation of software by users is established;

[b] installation of software by users is controlled based on the established policy; and

[c] installation of software by users is monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing user installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user-installed software; system monitoring records; system audit logs and records; continuous monitoring strategy; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for governing user-installed software; personnel operating, using, or maintaining the system; personnel monitoring compliance with user-installed software policy; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes governing user-installed software on the system; mechanisms enforcing rules or methods for governing the installation of software by users; mechanisms monitoring policy compliance].

DISCUSSION [NIST SP 800-171 R2]

Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved "app stores." Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

FURTHER DISCUSSION

Software that users have the ability to install is limited to items that the organization approves. When not controlled, users could install software that can create unnecessary risk. This risk applies both to the individual machine and to the larger operating environment. Policies and technical controls reduce risk to the organization by preventing users from installing unauthorized software.

Example

You are a system administrator. A user calls you for help installing a software package. They are receiving a message asking for a password because they do not have permission to install the software. You explain that the policy prohibits users from installing software without approval [a]. When you set up workstations for users, you do not provide administrative privileges. After the call, you redistribute the policy to all users ensuring everyone in the company is aware of the restrictions.

Potential Assessment Considerations

- Are user controls in place to prohibit the installation of unauthorized software [a]?[36]
- Is all software in use on the information systems approved [b]?[37]
- Is there a mechanism in place to monitor the types of software a user is permitted to download (e.g., is there a white list of approved software) [c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.4.9

[36] NIST Handbook 162 Section 3.4.9
[37] NIST Handbook 162 Section 3.4.9

Identification and Authentication (IA)

Level 1 IA Practices

IA.L1-3.5.1 – IDENTIFICATION

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] system users are identified;

[b] processes acting on behalf of users are identified; and

[c] devices accessing the system are identified.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers].

Test

[SELECT FROM: Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability].

DISCUSSION [NIST SP 800-171 R2]

Common device identifiers include media access control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring

identification may be defined by type, by device, or by a combination of type/device. NIST SP 800-63-3 provides guidance on digital identities.

FURTHER DISCUSSION

Make sure to assign individual, unique identifiers (e.g., user names) to all users and processes that access company systems. Authorized devices also should have unique identifiers. Unique identifiers can be as simple as a short set of alphanumeric characters (e.g., SW001 could refer to a network switch, SW002 could refer to a different network switch).

This practice, IA.L1-3.5.1, provides a vetted and trusted identity that supports the access control mechanism required by AC.L1-3.1.1.

Example

You want to make sure that all employees working on a project can access important information about it. Because this is work for the DoD and may contain FCI, you also need to prevent employees who are not working on that project from being able to access the information. You assign each employee is assigned a unique user ID, which they use to log into the system [a].

Potential Assessment Considerations

- Are unique identifiers issued to individual users (e.g., usernames) [a]?
- Are the processes and service accounts that an authorized user initiates identified (e.g., scripts, automatic updates, configuration updates, vulnerability scans) [b]?
- Are unique device identifiers used for devices that access the system identified [c]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.v
- NIST SP 800-171 Rev 2 3.5.1

IA.L1-3.5.2 – AUTHENTICATION

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the identity of each user is authenticated or verified as a prerequisite to system access;

[b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and

[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms supporting or implementing authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for

temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

NIST SP 800-63-3 provides guidance on digital identities.

FURTHER DISCUSSION

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

Some devices ship with default usernames and passwords. For example, some devices ship so that when you first log on to the device, the username is "admin" and the password is "admin". When you have devices with this type of default username and password, immediately change the default password to a unique password you create. Default passwords may be well known to the public, easily found in a search, or easy to guess, allowing an unauthorized person to access your system.

Example 1

You are in charge of purchasing. You know that some laptops come with a default username and password. You notify IT that all default passwords should be reset prior to laptop use [a]. You ask IT to explain the importance of resetting default passwords and convey how easily they are discovered using internet searches during next week's cybersecurity awareness training.

Example 2

Your company decides to use cloud services for email and other capabilities. Upon reviewing this practice, you realize every user or device that connects to the cloud service must be authenticated. As a result, you work with your cloud service provider to ensure that only properly authenticated users and devices are allowed to connect to the system [a,c].

Potential Assessment Considerations

- Are unique authenticators used to verify user identities (e.g., passwords) [a]?
- An example of a process acting on behalf of users could be a script that logs in as a person or service account [b]. Can the contractor show that it maintains a record of all of those service accounts for use when reviewing log data or responding to an incident?
- Are user credentials authenticated in system processes (e.g., credentials binding, certificates, tokens) [b]?
- Are device identifiers used in authentication processes (e.g., MAC address, non-anonymous computer name, certificates) [c]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.vi
- NIST SP 800-171 Rev 2 3.5.2

Level 2 IA Practices

IA.L2-3.5.3 – MULTIFACTOR AUTHENTICATION

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] privileged accounts are identified;

[b] multifactor authentication is implemented for local access to privileged accounts;

[c] multifactor authentication is implemented for network access to privileged accounts; and

[d] multifactor authentication is implemented for network access to non-privileged accounts.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms supporting or implementing authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the

application level, when necessary, to provide increased information security. Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.

NIST SP 800-63-3 provides guidance on digital identities.

FURTHER DISCUSSION

Implement a combination of two or more factors of authentication to verify privileged account holders' identity regardless of how the user is accessing the account. Implement a combination of two or more factors for non-privileged users accessing the system over a network.

The implementation of multi-factor authentication will depend on the environment and business needs. Although two-factor authentication directly on the computer is most common, there are situations (e.g., multi-factor identification for a mission system that cannot be altered) where additional technical or physical solutions can provide security. Multifactor authentication is not required for access to mobile devices such as smartphones or tablets – which are not considered to be network devices or information systems.

This practice, IA.L2-3.5.3, requires multifactor authentication for network access to non-privileged accounts and complements five other practices dealing with remote access (AC.L2-3.1.12, AC.L2-3.1.14, AC.L2-3.1.13, AC.L2-3.1.15, and MA.L2-3.7.5:

- AC.L2-3.1.12 requires the control of remote access sessions.
- AC.L2-3.1.14 limits remote access to specific access control points.
- AC.L2-3.1.13 requires the use of cryptographic mechanisms when enabling remote sessions.
- AC.L2-3.1.15 requires authorization for privileged commands executed during a remote.
- Finally, MA.L2-3.7.5 requires the addition of multifactor authentication for remote maintenance sessions.

This practice, IA.L2-3.5.3, also enhances IA.L1-3.5.2, which is a requirement for a less rigorous form of user authentication.

Example

You decide to implement multifactor authentication (MFA) to improve security of your network. Your first step is enabling MFA on VPN access to your internal network [c,d]. When users initiate remote access, they will be prompted for the additional authentication factor.

Because you also use a cloud-based email solution, you require MFA for access to that resource as well [c,d]. Finally, you enable MFA for both local and network logins for the system administrator accounts used to patch and manage servers [a,b,c].

Potential Assessment Considerations

- Does the system uniquely identify and authenticate users, including privileged accounts [b,c,d]?[38]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.3

[38] NIST Handbook 162 Section 3.5.3

IA.L2-3.5.4 – REPLAY-RESISTANT AUTHENTICATION

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of privileged system accounts; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting or implementing identification and authentication capability or replay resistant authentication mechanisms].

DISCUSSION [NIST SP 800-171 R2]

Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

NIST SP 800-63-3 provides guidance on digital identities.

FURTHER DISCUSSION

When insecure protocols are used for access to computing resources, an adversary may be able to capture login information and immediately reuse (replay) it for other purposes. It is important to use mechanisms that resist this technique.

Example

To protect your IT infrastructure, you understand that the methods for authentication must not be easily copied and re-sent to your systems by an adversary. You select Kerberos for authentication because of its built-in resistance to replay attacks. As a next step you upgrade all of your web applications to require Transport Layer Security (TLS), which also is replay-resistant. Your use of MFA to protect remote access also confers some replay resistance.

Potential Assessment Considerations

- Are only anti-replay authentication mechanisms used [a]?[39]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.4

[39] NIST Handbook 162 Section 3.5.4

IA.L2-3.5.5 – IDENTIFIER REUSE

Prevent reuse of identifiers for a defined period.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a period within which identifiers cannot be reused is defined; and

[b] reuse of identifiers is prevented within the defined period.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms supporting or implementing authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

Identifiers are provided for users, processes acting on behalf of users, or devices (IA.L1-3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

FURTHER DISCUSSION

Identifiers uniquely associate a user ID to an individual, group, role, or device. Establish guidelines and implement mechanisms to prevent identifiers from being reused for the period of time established in the policy.

Example

As a system administrator, you maintain a central directory/domain that holds the accounts for users, computers, and network devices. As part of your job, you issue unique usernames

(e.g., riley@acme.com) for the staff to access resources. When you issue staff computers you also rename the computer to reflect to whom it is assigned (e.g., riley-laptop01). Riley has recently left the organization, so you must manage the former staff member's account. Incidentally, their replacement is also named Riley. In the directory, you do not assign the previous account to the new user, as policy has defined an identifier reuse period of 24 months [a]. In accordance with policy, you create an account called riley02 [b]. This account is assigned the appropriate permissions for the new user. A new laptop is also provided with the identifier of riley02-laptop01.

Potential Assessment Considerations

- Are accounts uniquely assigned to employees, contractors, and subcontractors [b]?[40]
- Are account identifiers reused [b]?[41]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.5

[40] NIST Handbook 162 Section 3.5.5
[41] NIST Handbook 162 Section 3.5.5

IA.L2-3.5.6 – IDENTIFIER HANDLING

Disable identifiers after a defined period of inactivity.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a period of inactivity after which an identifier is disabled is defined; and

[b] identifiers are disabled after the defined period of inactivity.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records].

Interview

[SELECT FROM: Personnel with identifier management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting or implementing identifier management].

DISCUSSION [NIST SP 800-171 R2]

Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.

FURTHER DISCUSSION

Identifiers are uniquely associated with an individual, account, process, or device. An inactive identifier is one that has not been used for a defined extended period of time. For example, a user account may be needed for a certain time to allow for transition of business processes to existing or new staff. Once use of the identifier is no longer necessary, it should be disabled as soon as possible. Failure to maintain awareness of accounts that are no longer needed yet still active could allow an adversary to exploit IT services.

Example

One of your responsibilities is to enforce your company's inactive account policy: any account that has not been used in the last 45 days must be disabled [a]. You enforce this by writing a script that runs once a day to check the last login date for each account and generates a report of the accounts with no login records for the last 45 days. After reviewing the report, you notify each inactive employee's supervisor and disable the account [b].

Potential Assessment Considerations

- Are user accounts or identifiers monitored for inactivity [b]?[42]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.6

[42] NIST Handbook 162 Section 3.5.6

IA.L2-3.5.7 – PASSWORD COMPLEXITY

Enforce a minimum password complexity and change of characters when new passwords are created.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] password complexity requirements are defined;

[b] password change of character requirements are defined;

[c] minimum password complexity requirements as defined are enforced when new passwords are created; and

[d] minimum password change of character requirements as defined are enforced when new passwords are created.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms supporting or implementing authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

FURTHER DISCUSSION

Password complexity means using different types of characters as well as a specified number of characters. This applies to both the creation of new passwords and the modification of existing passwords. Characters to manage complexity include numbers, lowercase and uppercase letters, and symbols. Minimum complexity requirements are left up to the organization to define. Define the lowest level of password complexity required. Define the number of characters that must be changed when an existing password is changed. Enforce these rules for all passwords. Salting passwords adds a string of random characters (salt) to a password prior to hashing. This ensures the randomness of the resulting hash value.

Example

You work with management to define password complexity rules and ensure they are listed in the company's security policy. You define and enforce a minimum number of characters for each password and ensure that a certain number of characters must be changed when updating passwords [a,b]. Characters include numbers, lowercase and uppercase letters, and symbols [a]. These rules help create hard-to-guess passwords, which help to secure your network.

Potential Assessment Considerations

- Is a degree of complexity specified for passwords, (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 [a,b,c]?
- Is a change of characters required when new passwords are created [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.7

IA.L2-3.5.8 – PASSWORD REUSE

Prohibit password reuse for a specified number of generations.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the number of generations during which a password cannot be reused is specified and

[b] reuse of passwords is prohibited during the specified number of generations.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; password configurations and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting or implementing password-based authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

Password lifetime restrictions do not apply to temporary passwords.

FURTHER DISCUSSION

Individuals may not reuse their passwords for a defined period of time and a set number of passwords generated.

Example

You explain in your company's security policy that changing passwords regularly provides increased security by reducing the ability of adversaries to exploit stolen or purchased passwords over an extended period. You define how often individuals can reuse their passwords and the minimum number of password generations before reuse [a]. If a user tries to reuse a password before the number of password generations has been exceeded, an error message is generated, and the user is required to enter a new password [b].

Potential Assessment Considerations

- How many generations of password changes need to take place before a password can be reused [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.8

IA.L2-3.5.9 – TEMPORARY PASSWORDS

Allow temporary password use for system logons with an immediate change to a permanent password.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] an immediate change to a permanent password is required when a temporary password is used for system logon.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting or implementing password-based authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

FURTHER DISCUSSION

Users must change their temporary passwords the first time they log in. Temporary passwords often follow a consistent style within an organization and can be more easily guessed than passwords created by the unique user. This approach to temporary passwords should be avoided.

Example

One of your duties as a systems administrator is to create accounts for new users. You configure all systems with user accounts to require users to change a temporary password

upon initial login to a permanent password [a]. When a user logs on for the first time, they are prompted to create a unique password that meets all of the defined complexity rules.

Potential Assessment Considerations

- Are temporary passwords only valid to allow a user to perform a password reset [a]?
- Does the system enforce an immediate password change after logon when a temporary password is issued [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.9

IA.L2-3.5.10 – CRYPTOGRAPHICALLY-PROTECTED PASSWORDS

Store and transmit only cryptographically-protected passwords.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] passwords are cryptographically protected in storage; and

[b] passwords are cryptographically protected in transit.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms supporting or implementing authenticator management capability].

DISCUSSION [NIST SP 800-171 R2]

Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords.

See NIST Cryptographic Standards and Guidelines.

FURTHER DISCUSSION

All passwords must be cryptographically protected using a one-way function for storage and transmission. This type of protection changes passwords into another form, or a hashed password. A one-way transformation makes it theoretically impossible to turn the hashed password back into the original password, but inadequate complexity (IA.L2-3.5.7) may still facilitate offline cracking of hashes.

Example

You are responsible for managing passwords for your organization. You protect all passwords with a one-way transformation, or hashing, before storing them. Passwords are never transmitted across a network unencrypted [a,b].

Potential Assessment Considerations

- Are passwords prevented from being stored in reversible encryption form in any company systems [a]?[43]
- Are passwords stored as one-way hashes constructed from passwords [a]?[44]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.10

[43] NIST Handbook 162 Section 3.5.10
[44] NIST Handbook 162 Section 3.5.10

IA.L2-3.5.11 – OBSCURE FEEDBACK

Obscure feedback of authentication information.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authentication information is obscured during the authentication process.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing authenticator feedback; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; system or network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting or implementing the obscuring of feedback of authentication information during authentication].

DISCUSSION [NIST SP 800-171 R2]

The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

FURTHER DISCUSSION

Authentication information includes passwords. When users enter a password, the system displays a symbol, such as an asterisk, to obscure feedback preventing others from seeing the actual characters. Feedback is obscured based on a defined policy (e.g., smaller devices may briefly show characters before obscuring).

Example

As a system administrator, you configure your systems to display an asterisk when users enter their passwords into a computer system [a]. For mobile devices, the password characters are briefly displayed to the user before being obscured. This prevents people from figuring out passwords by looking over someone's shoulder.

Potential Assessment Considerations

- Is the feedback immediately obscured when the authentication is presented on a larger display (e.g., desktop or notebook computers with relatively large monitors) [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.5.11

Incident Response (IR)

Level 2 IR Practices

IR.L2-3.6.1 – INCIDENT HANDLING

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] an operational incident-handling capability is established;

[b] the operational incident-handling capability includes preparation;

[c] the operational incident-handling capability includes detection;

[d] the operational incident-handling capability includes analysis;

[e] the operational incident-handling capability includes containment;

[f] the operational incident-handling capability includes recovery; and

[g] the operational incident-handling capability includes user response activities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing incident response assistance; incident response plan; contingency plan; system security plan; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response training records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with incident response assistance and support responsibilities; personnel with access to incident response support and assistance capability; personnel with information security responsibilities].

Test

[SELECT FROM: Incident-handling capability for the organization; organizational processes for incident response assistance; mechanisms supporting or implementing incident response assistance].

DISCUSSION [NIST SP 800-171 R2]

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

NIST SP 800-61 provides guidance on incident handling. SP 800-86 and SP 800-101 provide guidance on integrating forensic techniques into incident response. SP 800-161 provides guidance on supply chain risk management.

FURTHER DISCUSSION

Incident handling capabilities prepare your organization to respond to incidents and may:

- identify people inside and outside your organization you may need to contact during an incident;
- establish a way to report incidents, such as an email address or a phone number;
- establish a system for tracking incidents; and
- determine a place and a way to store evidence of an incident.

Software and hardware may be required to analyze incidents when they occur. Incident prevention activities are also part of an incident-handling capability. The incident-handling team provides input for such things as risk assessments and training.

Contractors detect incidents using different indicators. Indicators may include:

- alerts from sensors or antivirus software;
- a filename that looks unusual; and

- log entries that raise concern.

After detecting an incident, an incident response team performs analysis. This requires some knowledge of normal network operations. The incident should be documented including all the log entries associated with the incident.

Containment of the incident is a critical step to stop the damage the incident is causing to your network. Containment activities should be based on previously defined organizational priorities and assessment of risk.

Recovery activities restore systems to pre-incident functionality and address its underlying causes. Organizations should use recovery activities as a means of improving their overall resilience to future attacks.

Example

Your manager asks you to set up your company's incident-response capability [a]. First, you create an email address to collect information on possible incidents. Next, you draft a contact list of all the people who need to know when an incident occurs. You document a procedure for how to submit incidents that includes roles and responsibilities when a potential incident is detected or reported. The procedure also explains how to track incidents, from initial creation to closure [b].

Potential Assessment Considerations

- Is there an incident response policy which specifically outlines requirements for handling of incidents involving CUI [a]?[45]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.6.1

[45] NIST Handbook 162 Section 3.6.1

IR.L2-3.6.2 – INCIDENT REPORTING

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] incidents are tracked;

[b] incidents are documented;

[c] authorities to whom incidents are to be reported are identified;

[d] organizational officials to whom incidents are to be reported are identified;

[e] identified authorities are notified of incidents; and

[f] identified organizational officials are notified of incidents.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with incident monitoring responsibilities; personnel with incident reporting responsibilities; personnel who have or should have reported incidents; personnel (authorities) to whom incident information is to be reported; personnel with information security responsibilities].

Test

[SELECT FROM: Incident monitoring capability for the organization; mechanisms supporting or implementing tracking and documenting of system security incidents; organizational processes for incident reporting; mechanisms supporting or implementing incident reporting].

DISCUSSION [NIST SP 800-171 R2]

Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator

reports. Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include 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, Executive Orders, directives, regulations, and policies.

NIST SP 800-61 provides guidance on incident handling.

FURTHER DISCUSSION

Incident handling is the actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred. The majority of the process consists of incident identification, containment, eradication, and recovery. During this process, it is essential to track the work processes required in order to effectively respond. Designate a central hub to serve as the point to coordinate, communicate, and track activities. The hub should receive and document information from system administrators, incident handlers, and others involved throughout the process. As the incident process moves toward eradication, executives, affected business units, and any required external stakeholders should be kept aware of the incident in order to make decisions affecting the business. Report to designated authorities, taking into account applicable laws, directives, regulations, and other guidance. Specify staff responsible for communicating about the incident to internal and external stakeholders.

Example

You notice unusual activity on a server and determine a potential security incident has occurred. You open a tracking ticket with the Security Operations Center (SOC), which assigns an incident handler to work the ticket [a]. The handler investigates and documents initial findings, which lead to a determination that unauthorized access occurred on the server [b]. The SOC establishes an incident management team consisting of security, database, network, and system administrators. The team meets daily to update progress and plan courses of action to contain the incident [a]. At the end of the day, the team provides a status report to IT executives [d,f]. Two days later, the team declares the incident contained. The team produces a final report as the database system is rebuilt and placed back into operation.

Potential Assessment Considerations

- Is there an incident response policy that directs the establishment of requirements for tracking and reporting of incidents involving CUI to appropriate officials [a,d]?
- Is cybersecurity incident information promptly reported to management [e,f]?[46]

[46] NIST Handbook 162 Section 3.6.2

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.6.2

IR.L2-3.6.3 – INCIDENT RESPONSE TESTING

Test the organizational incident response capability.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the incident response capability is tested.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with incident response testing responsibilities; personnel with information security responsibilities; personnel with responsibilities for testing plans related to incident response].

Test

[SELECT FROM: Mechanisms and processes for incident response].

DISCUSSION [NIST SP 800-171 R2]

Organizations 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 (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

NIST SP 800-84 provides guidance on testing programs for information technology capabilities.

FURTHER DISCUSSION

Testing incident response capability validates existing plans and highlights potential deficiencies. The test should address questions such as what happens during an incident; who is responsible for incident management; what tasks are assigned within the IT organization; what support is needed from legal, public affairs, or other business components; how resources are added if needed during the incident; and how law

enforcement is involved. Any negative impacts to the normal day-to-day operations when responding to an incident should also be identified and documented.

Example

You decide to conduct an incident response table top exercise that simulates an attacker gaining access to the network through a compromised server. You include relevant IT staff such as security, database, network, and system administrators as participants. You also request representatives from legal, human resources, and communications. You provide a scenario to the group and have prepared key questions aligned with the response plans to guide the exercise. During the exercise, you focus on how the team executes the incident response plan. Afterward, you conduct a debrief with everyone that was involved to provide feedback and develop improvements to the incident response plan [a].

Potential Assessment Considerations

- Does the incident response policy outline requirements for regular incident response plan testing and reviews of incident response capabilities [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.6.3

Maintenance (MA)

Level 2 MA Practices

MA.L2-3.7.1 – PERFORM MAINTENANCE

Perform maintenance on organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] system maintenance is performed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators].

Test

[SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

DISCUSSION [NIST SP 800-171 R2]

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

FURTHER DISCUSSION

One common form of computer security maintenance is regular patching of discovered vulnerabilities in software and operating systems, though there are others that require attention.

System maintenance includes:

- corrective maintenance (e.g., repairing problems with the technology);
- preventative maintenance (e.g., updates to prevent potential problems);
- adaptive maintenance (e.g., changes to the operative environment); and
- perfective maintenance (e.g., improve operations).

Example

You are responsible for maintenance activities on your company's machines. This includes regular planned maintenance, unscheduled maintenance, reconfigurations when required, and damage repairs [a]. You know that failing to conduct maintenance activities can impact system security and availability, so you ensure that maintenance is regularly performed. You track all maintenance performed to assist with troubleshooting later if needed.

Potential Assessment Considerations

- Are systems, devices, and supporting systems maintained per manufacturer recommendations or company defined schedules [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.7.1

MA.L2-3.7.2 – SYSTEM MAINTENANCE CONTROL

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] tools used to conduct system maintenance are controlled;

[b] techniques used to conduct system maintenance are controlled;

[c] mechanisms used to conduct system maintenance are controlled; and

[d] personnel used to conduct system maintenance are controlled.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

DISCUSSION [NIST SP 800-171 R2]

This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software,

and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

FURTHER DISCUSSION

Tools used to perform maintenance must remain secure so they do not introduce viruses or other malware into your system. Controlling your maintenance techniques prevents intentional or unintentional harm to your network and systems. Additionally, the personnel responsible for maintenance activities should be supervised considering their elevated privilege on company assets.

Example

You are responsible for maintenance activities on your company's machines. To avoid introducing additional vulnerability into the systems you are maintaining, you make sure that all maintenance tools are approved and their usage is monitored and controlled [a,b]. You ensure the tools are kept current and up-to-date [a]. You and your backup are the only people authorized to use these tools and perform system maintenance [d].

Potential Assessment Considerations

- Are physical or logical access controls used to limit access to maintenance tools to authorized personnel [a]?
- Are physical or logical access controls used to limit access to system documentation and organizational maintenance process documentation to authorized personnel [b]?
- Are physical or logical access controls used to limit access to automated mechanisms (e.g., automated scripts, scheduled jobs) to authorized personnel [c]?
- Are physical or logical access controls used to limit access to the system entry points that enable maintenance (e.g., administrative portals, local and remote console access, and physical equipment panels) to authorized personnel [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.7.2

MA.L2-3.7.3 – EQUIPMENT SANITIZATION

Ensure equipment removed for off-site maintenance is sanitized of any CUI.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators].

Test

[SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

DISCUSSION [NIST SP 800-171 R2]

This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

NIST SP 800-88 provides guidance on media sanitization.

FURTHER DISCUSSION

Sanitization is a process that makes access to data infeasible on media such as a hard drive. The process may overwrite the entire media with a fixed pattern such as binary zeros. In addition to clearing the data an organization could purge (e.g., degaussing, secure erasing, or disassembling) the data, or even destroy the media (e.g., incinerating, shredding, or

pulverizing). Performing one of these activities ensures that the data is extremely hard to recover, thus ensuring its confidentiality.

For additional guidance on which specific sanitization actions should be taken on any specific type of media, review the description of the Purge actions given in NIST SP 800-88 Revision 1 – Guidelines for Media Sanitization.

Example

You manage your organization's IT equipment. A recent DoD project has been using a storage array to house CUI. Recently, the array has experienced disk issues. After troubleshooting with the vendor, they recommend several drives be replaced in the array. Knowing the drives may contain CUI, you reference NIST 800-88 Rev. 1 and determine a strategy you can implement on the defective equipment – processing the drives with a degaussing unit [a]. Once all the drives have been wiped, you document the action and ship the faulty drives to the vendor.

Potential Assessment Considerations

- Is there a process for sanitizing (e.g., erasing, wiping, degaussing) equipment that was used to store, process, or transmit CUI before it is removed from the facility for off-site maintenance (e.g., manufacturer or contracted maintenance support) [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.7.3

MA.L2-3.7.4 – MEDIA INSPECTION

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

DISCUSSION [NIST SP 800-171 R2]

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

FURTHER DISCUSSION

As part of troubleshooting, a vendor may provide a diagnostic application to install on a system. As this is executable code, there is a chance that the file is corrupt or infected with malicious code. Implement procedures to scan any files prior to installation. The same level of scrutiny must be made as with any file a staff member may download.

This practice, MA.L2-3.7.4, extends both SI.L1-3.14.2 and SI.L1-3.14.4. SI.L1-3.14.2 and SI.L1-3.14.4 require the implementation and updating of mechanisms to protect systems from malicious code, and MA.L2-3.7.4 extends this requirement to diagnostic and testing tools.

Example

You have recently been experiencing performance issues on one of your servers. After troubleshooting for much of the morning, the vendor has asked to install a utility that will collect more data from the server. The file is stored on the vendor's FTP server. The support technician gives you the FTP site so you can anonymously download the utility file. You also ask him for a hash of the utility file. As you download the file to your local computer, you realize it is compressed. You unzip the file and perform a manual antivirus scan, which reports no issues [a]. To verify the utility file has not been altered, you run an application to see that the hash from the vendor matches.

Potential Assessment Considerations

- Are media containing diagnostic and test programs (e.g., downloaded or copied utilities or tools from manufacturer, third-party, or in-house support teams) checked for malicious code (e.g., using antivirus or antimalware scans) before the media are used on organizational systems [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.7.4

MA.L2-3.7.5 – NONLOCAL MAINTENANCE

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] multifactor authentication is used to establish nonlocal maintenance sessions via external network connections; and

[b] nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System maintenance policy; procedures addressing nonlocal system maintenance; system security plan; system design documentation; system configuration settings and associated documentation; maintenance records; diagnostic records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for managing nonlocal maintenance; mechanisms implementing, supporting, and managing nonlocal maintenance; mechanisms for strong authentication of nonlocal maintenance diagnostic sessions; mechanisms for terminating nonlocal maintenance sessions and network connections].

DISCUSSION [NIST SP 800-171 R2]

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA.L2-3.5.3.

FURTHER DISCUSSION

Nonlocal maintenance activities must use multifactor authentication. Multifactor authentication requires at least two factors, such as:

- something you know (e.g., password, personal identification number [PIN]);
- something you have (e.g., cryptographic identification device, token); or
- something you are (e.g., biometric fingerprint or facial scan).

Requiring two or more factors to prove your identity increases the security of the connection. Nonlocal maintenance activities are activities conducted from external network connections such as over the internet. After nonlocal maintenance activities are complete, shut down the external network connection.

This practice, MA.L2-3.7.5 requires the addition of multifactor authentication for remote maintenance sessions and complements five other practices dealing with remote access (AC.L2-3.1.12, AC.L2-3.1.14, AC.L2-3.1.13, AC.L2-3.1.15, and IA.L2-3.5.3):

- AC.L2-3.1.12 requires the control of remote access sessions.
- AC.L2-3.1.14 limits remote access to specific access control points.
- AC.L2-3.1.13 requires the use of cryptographic mechanisms when enabling remote sessions.
- AC.L2-3.1.15 requires authorization for privileged commands executed during a remote session.
- Finally, IA.L2-3.5.3 requires multifactor authentication for network access to non-privileged accounts.

Example

You are responsible for maintaining your company's firewall. In order to conduct maintenance while working remotely, you connect to the firewall's management interface and log in using administrator credentials. The firewall then sends a verification request to the multifactor authentication app on your smartphone [a]. You need both of these things to prove your identity [a]. After you respond to the multifactor challenge, you have access to the maintenance interface. When you finish your activities, you shut down the remote connection by logging out and quitting your web browser [b].

Potential Assessment Considerations

- Is multifactor authentication required prior to maintenance of a system when connecting remotely from outside the system boundary [a]?
- Are personnel required to manually terminate remote maintenance sessions established via external network connections when maintenance is complete, or are connections terminated automatically through system session management mechanisms [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.7.5

MA.L2-3.7.6 – MAINTENANCE PERSONNEL

Supervise the maintenance activities of maintenance personnel without required access authorization.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] maintenance personnel without required access authorization are supervised during maintenance activities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while PE.L1-3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

FURTHER DISCUSSION

Individuals without proper permissions must be supervised while conducting maintenance on organizational machines. Consider creating temporary accounts with short-term expiration periods rather than regular user accounts. Additionally, limit the permissions and access these accounts have to the most restrictive settings possible.

Example

One of your software providers has to come on-site to update the software on your company's computers. You give the individual a temporary logon and password that expires in 12 hours and is limited to accessing only the computers necessary to complete the work [a]. This gives the technician access long enough to perform the update. You monitor the individual's physical and network activity while the maintenance is taking place [a] and revoke access when the job is done.

Potential Assessment Considerations

- Are there processes for escorting and supervising maintenance personnel without required access authorization (e.g., vendor support personnel, short-term maintenance contractors) during system maintenance [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.7.6

Media Protection (MP)

Level 1 MP Practices

MP.L1-3.8.3 – MEDIA DISPOSAL

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] system media containing FCI is sanitized or destroyed before disposal; and

[b] system media containing FCI is sanitized before it is released for reuse.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; applicable standards and policies addressing media sanitization; system security plan; media sanitization records; system audit logs and records; system design documentation; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with media sanitization responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for media sanitization; mechanisms supporting or implementing media sanitization].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. 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 released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization.

Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing FCI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for federal contract information. NIST SP 800-88 provides guidance on media sanitization.

FURTHER DISCUSSION

"Media" refers to a broad range of items that store information, including paper documents, disks, tapes, digital photography, USB drives, CDs, DVDs, and mobile phones. It is important to know what information is on media so that you can handle it properly. If there is FCI, you or someone in your company should either:

- shred or destroy the device before disposal so it cannot be read; or
- clean or purge the information, if you want to reuse the device.

See NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization*, for more information.

Example

As you pack for an office move, you find some old CDs in a file cabinet. You determine that one has information about an old project your company did for the DoD. You shred the CD rather than simply throwing it in the trash [a].

Potential Assessment Considerations

- Is all managed data storage erased, encrypted, or destroyed using mechanisms to ensure that no usable data is retrievable [a,b]?[47]

KEY REFERENCES

- FAR Clause 52.204-21 b.1.vii
- NIST SP 800-171 Rev 2 3.8.3

[47] NIST Handbook 162 Section 3.8.3

Level 2 MP Practices

MP.L2-3.8.1 – MEDIA PROTECTION

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] paper media containing CUI is physically controlled;

[b] digital media containing CUI is physically controlled;

[c] paper media containing CUI is securely stored; and

[d] digital media containing CUI is securely stored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].

DISCUSSION [NIST SP 800-171 R2]

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Access to CUI on system media can be limited by physically controlling such media, which includes 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.

NIST SP 800-111 provides guidance on storage encryption technologies for end user devices.

FURTHER DISCUSSION

CUI can be contained on two types of physical media:

- hardcopy (e.g., CD drives, USB drives, magnetic tape); and
- digital devices (e.g., CD drives, USB drives, video).

You should store physical media containing CUI in a secure location. This location should be accessible only to those people with the proper permissions. All who access CUI should follow the process for checking it out and returning it.

Example

Your company has CUI for a specific Army contract contained on a USB drive. You store the drive in a locked drawer, and you log it on an inventory [d]. You establish a procedure to check out the USB drive so you have a history of who is accessing it. These procedures help to maintain the confidentiality, integrity, and availability of the data.

Potential Assessment Considerations

- Is hardcopy media containing CUI handled only by authorized personnel according to defined procedures [a]?
- Is digital media containing CUI handled only by authorized personnel according to defined procedures [b]?
- Is paper media containing CUI physically secured (e.g., in a locked drawer or cabinet) [c]?
- Is digital media containing CUI securely stored (e.g., in access-controlled repositories) [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.1

MP.L2-3.8.2 – MEDIA ACCESS

Limit access to CUI on system media to authorized users.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] access to CUI on system media is limited to authorized users.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

DISCUSSION [NIST SP 800-171 R2]

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

FURTHER DISCUSSION

Limit physical access to CUI to people permitted to access CUI. Use locked or controlled storage areas and limit access to only those allowed to access CUI. Keep track of who accesses physical CUI in an audit log.

Example

Your company has CUI for a specific Army contract contained on a USB drive. In order to control the data, you establish specific procedures for handling the drive. You designate the project manager as the owner of the data and require anyone who needs access to the data to get permission from the data owner [a]. The data owner maintains a list of users that are

authorized to access the information. Before an authorized individual can get access to the USB drive that contains the CUI they have to fill out a log and check out the drive. When they are done with the data, they check in the drive and return it to its secure storage location.

Potential Assessment Considerations

- Is a list of users who are authorized to access the CUI contained on system media maintained [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.2

MP.L2-3.8.4 – MEDIA MARKINGS

Mark media with necessary CUI markings and distribution limitations.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] media containing CUI is marked with applicable CUI markings; and

[b] media containing CUI is marked with distribution limitations.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; procedures addressing media marking; physical and environmental protection policy and procedures; system security plan; list of system media marking security attributes; designated controlled areas; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media protection and marking responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for marking information media; mechanisms supporting or implementing media marking].

DISCUSSION [NIST SP 800-171 R2]

The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations.

FURTHER DISCUSSION

All media, hardcopy and digital, must be properly marked to alert individuals to the presence of CUI stored on the media. The National Archives and Records Administration (NARA) has published guidelines for labeling media of different sizes.[48]

MP.L2-3.8.8 requires that media have an identifiable owner, so organizations may find it desirable to include ownership information on the device label as well.

[48] NARA, *CUI Notice 2019-01: Controlled Unclassified Information (CUI) Coversheets and Labels*

Example

You were recently contacted by the project team for a new DoD program. The team said they wanted the CUI in use for the program to be properly protected. When speaking with them, you realize that most of the protections will be provided as part of existing enterprise cybersecurity capabilities. They also mentioned that the project team will use several USB drives to share specific data. You explain that the team must ensure the USB drives are externally marked to indicate the presence of CUI [a]. The project team labels the outside of each USB drive with an appropriate CUI label following NARA guidance [a]. Further, the labels indicate that distribution is limited to those employees supporting the DoD program [a].

Potential Assessment Considerations

- Are all media containing CUI identified [a,b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.4

MP.L2-3.8.5 – MEDIA ACCOUNTABILITY

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] access to media containing CUI is controlled; and

[b] accountability for media containing CUI is maintained during transport outside of controlled areas.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing media storage and media protection].

DISCUSSION [NIST SP 800-171 R2]

Controlled areas are areas or spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information. Controls to maintain accountability for media during transport include locked 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 external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

FURTHER DISCUSSION

CUI is protected in both physical and digital formats. Physical control can be accomplished using traditional concepts like restricted access to physical locations or locking papers in a desk or filing cabinet. The digitization of data makes access to CUI much easier. CUI can be stored and transported on magnetic disks, tapes, USB drives, CD-ROMs, and so on. This makes digital CUI data very portable. It is important for an organization to apply mechanisms to prevent unauthorized access to CUI due to ease of transport.

Example

Your team has recently completed configuring a server for a DoD customer. The customer has asked that it be ready to plug in and use. An application installed on the server contains data that is considered CUI. You box the server for shipment using tamper-evident packaging and label it with the specific recipient for the shipment [b]. You select a reputable shipping service so you will get a tracking number to monitor the progress. Once the item is shipped, you send the recipients the tracking number so they can monitor and ensure prompt delivery at their facility.

Potential Assessment Considerations

- Do only approved individuals have access to media containing CUI [a]?
- Is access to the media containing CUI recorded in an audit log [b]?
- Is all CUI data on media encrypted or physically locked prior to transport outside of secure locations [b]?[49]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.5

[49] NIST Handbook 162 Section 3.8.5

MP.L2-3.8.6 – PORTABLE STORAGE ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings and associated documentation; system media transport records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media transport responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives).

NIST SP 800-111 provides guidance on storage encryption technologies for end user devices.

FURTHER DISCUSSION

CUI can be stored and transported on a variety of portable media, which increases the chance that the CUI can be lost. When identifying the paths CUI flows through your company, identify devices to include in this practice.

To mitigate the risk of losing or exposing CUI, implement an encryption scheme to protect the data. Even if the media are lost, proper encryption renders the data inaccessible. When encryption is not an option, apply alternative physical safeguards during transport.

This practice, MP.L2-3.8.6, provides additional protections to those provided by MP.L2-3.8.5. This practice is intended to protect against situations where control of media access fails, such as through the loss of the media.

Example

You manage the backups for file servers in your datacenter. You know that in addition to the company's sensitive information, CUI is stored on the file servers. As part of a broader plan to protect data, you send the backup tapes off site to a vendor. You are aware that your backup software provides the option to encrypt data onto tape. You develop a plan to test and enable backup encryption for the data sent off site. This encryption provides additional protections for the data on the backup tapes during transport and offsite storage [a].

Potential Assessment Considerations

- Are all CUI data on media encrypted or physically protected prior to transport outside of controlled areas [a]?
- Are cryptographic mechanisms used to protect digital media during transport outside of controlled areas [a]?
- Do cryptographic mechanisms comply with FIPS 140-2 [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.6

MP.L2-3.8.7 – REMOVEABLE MEDIA

Control the use of removable media on system components.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the use of removable media on system components is controlled.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for media use; mechanisms restricting or prohibiting use of system media on systems or system components].

DISCUSSION [NIST SP 800-171 R2]

In contrast to requirement MP.L2-3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices. Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. Many 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 organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations 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 the functions intended.

FURTHER DISCUSSION

Removable media are any type of media storage that you can remove from your computer or machine (e.g., CDs, DVDs, diskettes, and USB drives). Write a specific policy for removable media. The policy should cover the various types of removable media (e.g., write-once media and rewritable media) and should discuss the company's approach to removable media. Ensure the following controls are considered and included in the policy:

- limit the use of removable media to the smallest number needed; and
- scan all removable media for viruses.

Example

You are in charge of IT operations. You establish a policy for removable media that includes USB drives [a]. The policy information such as:

- only USB drives issued by the organization may be used; and
- USB drives are to be used for work purposes only [a].

You set up a separate computer to scan these drives before anyone uses them on the network. This computer has anti-virus software installed that is kept up to date.

Potential Assessment Considerations

- Are removable media allowed [a]?[50]
- Are policies and/or procedures in use to control the use of removable media [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.7

[50] NIST Handbook 162 Section 3.8.7

MP.L2-3.8.8 – SHARED MEDIA

Prohibit the use of portable storage devices when such devices have no identifiable owner.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the use of portable storage devices is prohibited when such devices have no identifiable owner.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system configuration settings and associated documentation; system design documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for media use; mechanisms prohibiting use of media on systems or system components].

DISCUSSION [NIST SP 800-171 R2]

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

FURTHER DISCUSSION

A portable storage device is a system component that can be inserted into and removed from a system and is used to store data or information. It typically plugs into a laptop or desktop port (e.g., USB port). These devices can contain malicious files that can lead to a compromise of a connected system. Therefore, use should be prohibited if the device cannot be traced to an owner who is responsible and accountable for its security.

This practice, MP.L2-3.8.8, furthers the protections provided by MP.L2-3.8.7 by prohibiting unidentified media use even if that media type is allowable.

Example

You are the IT manager. One day, a staff member reports finding a USB drive in the parking lot. You investigate and learn that there are no labels on the outside of the drive to indicate who might be responsible for it. You send an email to all employees to remind them that IT policies expressly prohibit plugging unknown devices into company computers. You also direct staff members to turn in to the IT help desk any devices that have no identifiable owner [a].

Potential Assessment Considerations

- Do portable storage devices used have identifiable owners [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.8

MP.L2-3.8.9 – PROTECT BACKUPS

Protect the confidentiality of backup CUI at storage locations.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the confidentiality of backup CUI is protected at storage locations.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Procedures addressing system backup; system configuration settings and associated documentation; security plan; backup storage locations; system backup logs or records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system backup responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for conducting system backups; mechanisms supporting or implementing system backups].

DISCUSSION [NIST SP 800-171 R2]

Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backed-up information containing CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

FURTHER DISCUSSION

You protect CUI to ensure that it remains private (confidentiality) and unchanged (integrity). Methods to ensure confidentiality may include:

- encrypting files or media;
- managing who has access to the information; and
- physically securing devices and media that contain CUI.

Storage locations for information are varied, and may include:

- external hard drives;

- USB drives;
- magnetic media (tape cartridge);
- optical disk (CD, DVD);
- Networked Attached Storage (NAS);
- servers; and
- cloud backup.

This practice, MP.L2-3.8.9, requires the confidentiality of backup information at storage locations.

Example

You are in charge of protecting CUI for your company. Because the company's backups contain CUI, you work with IT to protect the confidentiality of backup data. You agree to encrypt all CUI data as it is saved to an external hard drive [a].

Potential Assessment Considerations

- Are data backups encrypted on media before removal from a secured facility [a]?
- Are cryptographic mechanisms FIPS validated [a]?[51]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.8.9

[51] NIST Handbook 162 Section 3.8.9

Personnel Security (PS)

Level 2 PS Practices

PS.L2-3.9.1 – SCREEN INDIVIDUALS

Screen individuals prior to authorizing access to organizational systems containing CUI.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] individuals are screened prior to authorizing access to organizational systems containing CUI.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with personnel security responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for personnel screening].

DISCUSSION [NIST SP 800-171 R2]

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

FURTHER DISCUSSION

Ensure all employees who need access to CUI undergo organization-defined screening before being granted access. Base the types of screening on the requirements for a given position and role.

The effective screening of personnel provided by this practice, PS.L2-3.9.1, improves upon the effectiveness of authentication performed in IA.L1-3.5.2.

Example

You are in charge of security at your organization. You complete standard criminal background and credit checks of all individuals you hire before they can access CUI [a]. Your screening program follows appropriate laws, policies, regulations, and criteria for the level of access required for each position.

Potential Assessment Considerations

- Are appropriate background checks completed prior granting access to organizational systems containing CUI [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.9.1

PS.L2-3.9.2 – PERSONNEL ACTIONS

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established;

[b] system access and credentials are terminated consistent with personnel actions such as termination or transfer; and

[c] the system is protected during and after personnel transfer actions.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked authenticators and credentials; records of exit interviews; other relevant documents or records].

Interview

[SELECT FROM: Personnel with personnel security responsibilities; personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for personnel transfer and termination; mechanisms supporting or implementing personnel transfer and termination notifications; mechanisms for disabling system access and revoking authenticators].

DISCUSSION [NIST SP 800-171 R2]

Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-

availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

FURTHER DISCUSSION

Employee access to CUI is removed when they change jobs or leave the company. When employment or program access is terminated for any reason, the following actions may occur within the defined time frame:

- all company IT equipment (e.g., laptops, cell phones, storage devices) is returned;
- all identification, access cards, and keys are returned; and
- an exit interview is conducted to remind the employee of their obligations to not discuss CUI, even after employment.

Additionally, perform the following:

- remove access to all accounts granting access to CUI or modify access to CUI as appropriate for a new work role;
- disable or close employee accounts for departing employees; and
- limit access to physical spaces with CUI for departing employees or those who transition to a work role that does not require access to CUI.

This practice, PS.L2-3.9.2, leverages the identification of system users required by IA.L1-3.5.1 in order to ensure that all accesses are identified and removed.

Example 1

You are in charge of IT operations. Per organizational policies, when workers leave the company, you remove them from any physical CUI access lists. If you are not their supervisor, you contact their supervisor or human resources immediately and ask them to:

- turn in the former employees' computers for proper handling;
- inform help desk or system administrators to have the former employees' system access revoked;
- retrieve the former employees' identification and access cards; and

- have the former employees attend an exit interview where you or human resources remind them of their obligations to not discuss CUI [b].

Example 2

An employee transfers from one working group in your company to another. Human resources team notifies IT of the transfer date, and the employee's new manager follows procedure by submitting a ticket to the IT help desk to provide information on the access rights the employee will require in their new role. IT implements the rights for the new position and revokes the access for the prior position on the official date of the transfer [c].

Potential Assessment Considerations

- Is information system access disabled upon employee termination or transfer [c]?
- Are authenticators/ credentials associated with the employee revoked upon termination or transfer within a certain time frame [b,c]?
- Is all company information system-related property retrieved from the terminated or transferred employee within a certain timeframe [a,c]?
- Is access to company information and information systems formerly controlled by the terminated or transferred employee retained for a certain timeframe [a,c]?
- Is the information security office and data owner of the change in authorization notified within a certain timeframe [a]?[52]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.9.2

[52] NIST Handbook 162 Section 3.9.2

Physical Protection (PE)

Level 1 PE Practices

PE.L1-3.10.1 – LIMIT PHYSICAL ACCESS

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized individuals allowed physical access are identified;

[b] physical access to organizational systems is limited to authorized individuals;

[c] physical access to equipment is limited to authorized individuals; and

[d] physical access to operating environments is limited to authorized individuals.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only, and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

FURTHER DISCUSSION

This addresses the company's physical space (e.g., office, testing environments, equipment rooms), technical assets, and non-technical assets that need to be protected from unauthorized physical access. Specific environments are limited to authorized employees, and access is controlled with badges, electronic locks, physical key locks, etc.

Output devices, such as printers, are placed in areas where their use does not expose data to unauthorized individuals. Lists of personnel with authorized access are developed and maintained, and personnel are issued appropriate authorization credentials.

Example

You manage a DoD project that requires special equipment used only by project team members [b,c]. You work with the facilities manager to put locks on the doors to the areas where the equipment is stored and used [b,c,d]. Project team members are the only individuals issued with keys to the space. This restricts access to only those employees who work on the DoD project and require access to that equipment.

Potential Assessment Considerations

- Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued [a]?[53]
- Has the facility/building manager designated building areas as "sensitive" and designed physical security protections (e.g., guards, locks, cameras, card readers) to limit physical access to the area to only authorized employees [b,c,d]?[54]
- Are output devices such as printers placed in areas where their use does not expose data to unauthorized individuals [c]?[55]

KEY REFERENCES

- FAR Clause 52.204-21 b.1.viii
- NIST SP 800-171 Rev 2 3.10.1

[53] NIST Handbook 162 Section 3.10.1
[54] NIST Handbook 162 Section 3.10.1
[55] NIST Handbook 162 Section 3.10.1

PE.L1-3.10.3 – ESCORT VISITORS

Escort visitors and monitor visitor activity.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] visitors are escorted; and

[b] visitor activity is monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records].

Interview

[SELECT FROM: Personnel with physical access control responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

DISCUSSION [NIST SP 800-171 R2]

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

FURTHER DISCUSSION

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

Example

Coming back from a meeting, you see the friend of a coworker walking down the hallway near your office. You know this person well and trust them, but are not sure why they are in the building. You stop to talk, and the person explains that they are meeting a coworker for

lunch, but cannot remember where the lunchroom is. You walk the person back to the reception area to get a visitor badge and wait until someone can escort them to the lunch room [a]. You report this incident and the company decides to install a badge reader at the main door so visitors cannot enter without an escort [a].

Potential Assessment Considerations

- Are personnel required to accompany visitors to areas in a facility with physical access to organizational systems [a]?
- Are visitors clearly distinguishable from regular personnel [b]?
- Is visitor activity monitored (e.g., use of cameras or guards, reviews of secure areas upon visitor departure, review of visitor audit logs) [b]?

KEY REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 Rev 2 3.10.3

PE.L1-3.10.4 – PHYSICAL ACCESS LOGS

Maintain audit logs of physical access.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] audit logs of physical access are maintained.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records].

Interview

[SELECT FROM: Personnel with physical access control responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

DISCUSSION [NIST SP 800-171 R2]

Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

FURTHER DISCUSSION

Make sure you have a record of who accesses your facility (e.g., office, plant, factory). You can do this in writing by having employees and visitors sign in and sign out or by electronic means such as badge readers. Whatever means you use, you need to retain the access records for the time period that your company has defined.

Example

You and your coworkers like to have friends and family join you for lunch at the office on Fridays. Your small company has just signed a contract with the DoD, however, and you now need to document who enters and leaves your facility. You work with the reception staff to ensure that all non-employees sign in at the reception area and sign out when they leave [a]. You retain those paper sign-in sheets in a locked filing cabinet for one year. Employees receive badges or key cards that enable tracking and logging access to company facilities.

Potential Assessment Considerations

- Are logs of physical access to sensitive areas (both authorized access and visitor access) maintained per retention requirements [a]?[56]
- Are visitor access records retained for as long as required [a]?[57]

KEY REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 Rev 2 3.10.4

[56] NIST Handbook 162 Section 3.10.4
[57] NIST Handbook 162 Section 3.10.4

PE.L1-3.10.5 – MANAGE PHYSICAL ACCESS

Control and manage physical access devices.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] physical access devices are identified;

[b] physical access devices are controlled; and

[c] physical access devices are managed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records].

Interview

[SELECT FROM: Personnel with physical access control responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

DISCUSSION [NIST SP 800-171 R2]

Physical access devices include keys, locks, combinations, and card readers.

FURTHER DISCUSSION

Identifying and controlling physical access devices (e.g., locks, badges, key cards) is just as important as monitoring and limiting who is able to physically access certain equipment. Physical access devices are only strong protection if you know who has them and what access they allow. Physical access devices can be managed using manual or automatic processes such a list of who is assigned what key, or updating the badge access system as personnel change roles.

Example

You are a facility manager. A team member retired today and returns their company keys to you. The project on which they were working requires access to areas that contain equipment with FCI. You receive the keys, check your electronic records against the serial numbers on the keys to ensure all have been returned, and mark each key returned [c].

Potential Assessment Considerations

- Are lists or inventories of physical access devices maintained (e.g., keys, facility badges, key cards) [a]?
- Is access to physical access devices limited (e.g., granted to, and accessible only by, authorized individuals) [b]?
- Are physical access devices managed (e.g., revoking key card access when necessary, changing locks as needed, maintaining access control devices and systems) [c]?

KEY REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 Rev 2 3.10.5

Level 2 PE Practices

PE.L2-3.10.2 – MONITOR FACILITY

Protect and monitor the physical facility and support infrastructure for organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the physical facility where organizational systems reside is protected;

[b] the support infrastructure for organizational systems is protected;

[c] the physical facility where organizational systems reside is monitored; and

[d] the support infrastructure for organizational systems is monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; system security plan; physical access logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records].

Interview

[SELECT FROM: Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for monitoring physical access; mechanisms supporting or implementing physical access monitoring; mechanisms supporting or implementing the review of physical access logs].

DISCUSSION [NIST SP 800-171 R2]

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support

infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

FURTHER DISCUSSION

The infrastructure inside of a facility, such as power and network cables, is protected so that visitors and unauthorized employees cannot access it. The protection is also monitored by security guards, video cameras, sensors, or alarms.

Example

You are responsible for protecting your IT facilities. You install video cameras at each entrance and exit, connect them to a video recorder, and show the camera feeds on a display at the reception desk [c,d]. You also make sure there are secure locks on all entrances, exits, and windows to the facilities [a,b].

Potential Assessment Considerations

- Is physical access monitored to detect and respond to physical security incidents [c, d]?[58]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.10.2

[58] NIST Handbook 162 Section 3.10.2

PE.L2-3.10.6 – ALTERNATIVE WORK SITES

Enforce safeguarding measures for CUI at alternate work sites.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] safeguarding measures for CUI are defined for alternate work sites; and

[b] safeguarding measures for CUI are enforced for alternate work sites.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for personnel; system security plan; list of safeguards required for alternate work sites; assessments of safeguards at alternate work sites; other relevant documents or records].

Interview

[SELECT FROM: Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel].

DISCUSSION [NIST SP 800-171 R2]

Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

NIST SP 800-46 and NIST SP 800-114 provide guidance on enterprise and user security when teleworking.

FURTHER DISCUSSION

Many people work from home or travel as part of their job. Define and implement safeguards to account for protection of information beyond the enterprise perimeter. Safeguards may include physical protections, such as locked file drawers, as well as electronic protections such as encryption, audit logging, and proper access controls.

Example

Many of your company's project managers work remotely as they often travel to sponsor locations or even work from home. Because the projects on which they work require access to CUI, you must ensure the same level of protection is afforded as when they work in the office. You ensure that each laptop is deployed with patch management and anti-virus software protection [b]. Because data may be stored on the local hard drive, you have enabled full-disk encryption on their laptops [b]. When a remote staff member needs access to the internal network you require VPN connectivity that also disconnects the laptop from the remote network (i.e., prevents split tunneling) [b]. The VPN requires multifactor authentication to verify remote users are who they claim to be [b].

Potential Assessment Considerations

- Do all alternate sites where CUI data is stored or processed meet the same physical security requirements as the main site [b]?[59]
- Does the alternate processing site provide information security measures equivalent to those of the primary site [b]?[60]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.10.6

[59] NIST Handbook 162 Section 3.10.6
[60] NIST Handbook 162 Section 3.10.6

Risk Assessment (RA)

Level 2 RA Practices

RA.L2-3.11.1 – RISK ASSESSMENTS

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined; and

[b] risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records].

Interview

[SELECT FROM: Personnel with risk assessment responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].

DISCUSSION [NIST SP 800-171 R2]

Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractor operating systems on behalf of the organization, individuals

accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

NIST SP 800-30 provides guidance on conducting risk assessments.

FURTHER DISCUSSION

Risk arises from anything that can reduce an organization's assurance of mission/business success; cause harm to image or reputation; or harm individuals, other organizations, or the Nation.

Organizations assess the risk to their operations and assets at regular intervals. Areas where weakness or vulnerabilities could lead to risk may include:

- poorly designed and executed business processes;
- inadvertent actions of people, such as disclosure or modification of information;
- intentional actions of people inside and outside the organization;
- failure of systems to perform as intended;
- failures of technology; and
- external events, such as natural disasters, public infrastructure and supply chain failures.

When conducting risk assessments use established criteria and procedures. The results of formal risk assessments are documented. It is important to note that risk assessments differ from vulnerability assessments (see RA.L2-3.11.2). A vulnerability assessment provides input to a risk assessment along with other information such as results from likelihood analysis and analysis of potential treat sources.

Risk assessments should be performed at defined regular intervals. Mission risks include anything that will keep an organization from meeting its mission. Function risk is anything that will prevent the performance of a function. Image and reputation risks refer to intangible risks that have value and could cause damage to potential or future trust relationships.[61]

This practice, RA.L2-3.11.1, which requires periodically assessing the risk to organization systems, assets, and individuals, is a baseline Risk Assessment practice. RA.L2-3.11.1 enables other Risk Assessment practices (e.g., RA.L2-3.11.3, Vulnerability Remediation), as well as CA.L2-3.12.2, Plan of Action.

Example

You are a system administrator. You and your team members are working on a big government contract requiring you to store CUI. As part of your periodic (e.g., annual) risk assessment exercise, you evaluate the new risk involved with storing CUI [a,b]. When conducting the assessment you consider increased legal exposure, financial requirements of safeguarding CUI, potentially elevated attention from external attackers, and other factors.

[61] NIST SP 800-30, *Guide for Conducting Risk Assessments*, September 2012.

After determining how storing CUI affects your overall risk profile, you use that as a basis for a conversation on how that risk should be mitigated.

Potential Assessment Considerations

- Have initial and periodic risk assessments been conducted [b]?[62]
- Are methods defined for assessing risk (e.g., reviewing security assessments, incident reports, and security advisories, identifying threat sources, threat events, and vulnerabilities, and determining likelihood, impact, and overall risk to the confidentiality of CUI) [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.11.1

[62] NIST Handbook 162 Section 3.11.1

RA.L2-3.11.2 – VULNERABILITY SCAN

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the frequency to scan for vulnerabilities in organizational systems and applications is defined;

[b] vulnerability scans are performed on organizational systems with the defined frequency;

[c] vulnerability scans are performed on applications with the defined frequency;

[d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified; and

[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].

DISCUSSION [NIST SP 800-171 R2]

Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new

vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers). Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

NIST SP 800-40 provides guidance on vulnerability management.

FURTHER DISCUSSION

A vulnerability scanner is an application that identifies vulnerabilities in organizational assets. Most scanners can create a prioritized list of vulnerabilities ordered by their level of severity. Scan for vulnerabilities on all devices connected to the network including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers. All assets that are within the scope of the CMMC assessment must be scanned, including assets such as laptop computers that may not routinely connect to an organization's network.

Perform reviews of your organization's custom-developed software. Vulnerability analysis of a custom-made solution may require a penetration tester to properly test and validate findings. Automated vulnerability scanners may not be as thorough when scanning custom developed applications. Source code scanners can help identify weaknesses and vulnerabilities within code prior to compilation and use.

The vulnerability scanning process is a regular activity, not a single occurrence. Organizations put in place a vulnerability scanner that updates its database each time it performs a scan so it can identify the most current known vulnerabilities. Schedule scans with consideration of the potential for impact to normal operations and use caution when scanning critical assets.

This practice, RA.L2-3.11.2, which ensures scanning for vulnerabilities in organizational systems and application, is a baseline Risk Assessment practice. RA.L2-3.11.2 ,contributes to performing risk assessments as described in RA.L2-3.11.1.

Example

You are a system administrator. Your organization has assessed its risk and determined that it needs to scan for vulnerabilities in systems and applications once each quarter [a]. You conduct some tests and decide that it is important to be able to schedule scans after standard business hours. You also realize that you have remote workers and that you will need to be sure to scan their remote computers as well [b]. After some final tests, you integrate the scans into normal IT operations, running as scheduled [b,c]. You verify that the scanner application receives the latest updates on vulnerabilities and that those are included in future scans [d,e].

Potential Assessment Considerations

- Is the frequency specified for vulnerability scans to be performed in organizational systems and applications (e.g., continuous passive scanning, scheduled active scans) [a]?
- Are vulnerability scans performed on a defined frequency or randomly in accordance with company policy [a,b,c]?[63]
- Are systems periodically scanned for common and new vulnerabilities [d,e]?[64]
- Is the list of scanned system vulnerabilities updated on a defined frequency or when new vulnerabilities are identified and reported [d,e]?[65]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.11.2

[63] NIST Handbook 162 Section 3.11.2
[64] NIST Handbook 162 Section 3.11.2
[65] NIST Handbook 162 Section 3.11.2

RA.L2-3.11.3 – VULNERABILITY REMEDIATION

Remediate vulnerabilities in accordance with risk assessments.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] vulnerabilities are identified; and

[b] vulnerabilities are remediated in accordance with risk assessments.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].

DISCUSSION [NIST SP 800-171 R2]

Vulnerabilities discovered, for example, via the scanning conducted in response to RA.L2-3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

FURTHER DISCUSSION

Not all vulnerabilities captured in a vulnerability scanner may pose the same level of risk to an organization. Prioritize mitigation efforts to close the most critical vulnerabilities first. Track all vulnerability remediation to ensure completion; also track vulnerabilities that you have determined not to remediate.

This practice, RA.L2-3.11.3, benefits from CA.L2-3.12.2. RA.L2-3.11.3 allows remediation of vulnerabilities to take place based on the developed plans of actions for vulnerabilities from CA.L2-3.12.2.

Example

You are a system administrator. Each quarter you receive a list of vulnerabilities generated by your company's vulnerability scanner [a]. You prioritize that list and note which vulnerabilities should be targeted as soon as possible as well as which vulnerabilities you can safely defer addressing at this time. You document the reasoning behind accepting the risk of the unremediated flaws and note to continue to monitor these vulnerabilities in case you need to revise the decision at a later date [b].

Potential Assessment Considerations

- Are the results of risk assessments used to prioritize vulnerabilities for remediation [b]?
- For any given vulnerability is action taken for remediation, acceptance, avoidance, or transference of the vulnerability risk [b]?[66]
- Are all high risk vulnerabilities prioritized [b]?[67]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.11.3

[66] NIST Handbook 162 Section 3.11.3
[67] NIST Handbook 162 Section 3.11.3

Security Assessment (CA)

Level 2 CA Practices

CA.L2-3.12.1 – SECURITY CONTROL ASSESSMENT

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the frequency of security control assessments is defined; and

[b] security controls are assessed with the defined frequency to determine if the controls are effective in their application.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security assessment responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].

DISCUSSION [NIST SP 800-171 R2]

Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the system life cycle.

NIST SP 800-53 provides guidance on security and privacy controls for systems and organizations. SP 800-53A provides guidance on developing security assessment plans and conducting assessments.

FURTHER DISCUSSION

Avoid a "set it and forget it" mentality when implementing security controls. The security landscape is constantly changing. Reassess existing controls at periodic intervals in order to validate their effectiveness in your environment. Set the assessment schedule according to organizational needs. Consider regulatory obligations and internal policies when assessing the controls.

Outputs from security control assessments typically include:

- documented assessment results;
- proposed new controls, or updates to existing controls;
- remediation plans; and
- newly identified risks.

This practice, CA.L2-3.12.1, which ensures determining security controls are implemented properly, promotes effective security assessments for organizational systems required by CA.L2-3.12.3.

Example

You are in charge of IT operations. You need to ensure that the security controls implemented within the system are achieving their objectives [b]. Taking the practices outlined in your SSP as a guide, you conduct annual written reviews of the security controls to ensure they meet your organization's needs. When you find controls that do not meet requirements, you propose updated or new controls, develop a written implementation plan, document new risks, and execute the changes.

Potential Assessment Considerations

- Are security controls assessed at least annually [a]?

- Is the output of the security controls assessment documented [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.12.1

CA.L2-3.12.2 – PLAN OF ACTION

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] deficiencies and vulnerabilities to be addressed by the plan of action are identified;

[b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities; and

[c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records].

Interview

[SELECT FROM: Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action].

DISCUSSION [NIST SP 800-171 R2]

The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

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 and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

FURTHER DISCUSSION

When you write a plan of action, define the clear goal or objective of the plan. You may include the following in the action plan:

- ownership of who is accountable for ensuring the plan's performance;
- specific steps or milestones that are clear and actionable;
- assigned responsibility for each step or milestone;
- milestones to measure plan progress; and
- completion dates.

This practice, CA.L2-3.12.2, which ensures developing and implementing plans of action to correct and reduce vulnerabilities in systems, is driven by risk management practice RA.L2-3.11.1, which promotes periodically assessing risk to organizational systems. CA.L2-3.12.2 promotes monitoring security controls on an ongoing basis as defined in practice CA.L2-3.12.3.

Example

As IT director, one of your duties is to develop action plans when you discover that your company is not meeting security requirements or when a security issue arises [b]. A recent vulnerability scan identified several items that need to be addressed so you develop a plan to fix them [b]. Your plan identifies the people responsible for fixing the issues, how to do it, and when the remediation will be completed [b]. You also define how to verify that the person responsible has fixed the vulnerability [b]. You document this in a plan of action that is updated as milestones are reached [b]. You have a separate resource review the modifications after they have been completed to ensure the plan has been implemented correctly [c].

Potential Assessment Considerations

- Is there an action plan to remediate identified weaknesses or deficiencies [a]?[68]
- Is the action plan maintained as remediation is performed [b]?[69]
- Does the action plan designate remediation dates and milestones for each item [c]?[70]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.12.2

[68] NIST Handbook 162 Section 3.12.2
[69] NIST Handbook 162 Section 3.12.2
[70] NIST Handbook 162 Section 3.12.2

CA.L2-3.12.3 – SECURITY CONTROL MONITORING

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security planning policy; organizational procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

DISCUSSION [NIST SP 800-171 R2]

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions. Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

NIST SP 800-137 provides guidance on continuous monitoring.

FURTHER DISCUSSION

Provide a plan for monitoring the state of security controls on a recurring basis that occurs more frequently than the periodic assessments discussed in CA.L2-3.12.1. This process provides a mechanism to assess the overall security posture of your organization, which directly relates to activities discussed in CA.L2-3.12.4. As a result, the process not only maintains awareness of vulnerabilities and threats, but it also informs management of the effectiveness of the security controls in determining if security controls are current and for management to make an acceptable risk decision.

Example

You are responsible for ensuring your company fulfills all cybersecurity requirements for its DoD contracts. You review those requirements and the security controls your company has put in place to meet them. You then create a plan to evaluate each control regularly over the next year. You mark several controls to be evaluated by a third-party security assessor. You assign other IT resources in the organization to evaluate controls within their area of responsibility. To ensure progress you establish recurring meetings with the accountable IT staff to assess continuous monitoring progress, review security information, evaluate risks from gaps in continuous monitoring, and produce reports for your management [a].

Potential Assessment Considerations

- Are the security controls that need to be continuously monitored identified [a]?
- Is the timeframe for continuous monitoring activities to support risk-based decision making defined [a]?
- Is the output of continuous monitoring activities provided to stakeholders [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.12.3

CA.L2-3.12.4 – SYSTEM SECURITY PLAN

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.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a system security plan is developed;

[b] the system boundary is described and documented in the system security plan;

[c] the system environment of operation is described and documented in the system security plan;

[d] the security requirements identified and approved by the designated authority as non-applicable are identified;

[e] the method of security requirement implementation is described and documented in the system security plan;

[f] the relationship with or connection to other systems is described and documented in the system security plan;

[g] the frequency to update the system security plan is defined; and

[h] system security plan is updated with the defined frequency.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

DISCUSSION [NIST SP 800-171 R2]

System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or

implementation of the controls. 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 if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

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 and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

NIST SP 800-18 provides guidance on developing security plans.

FURTHER DISCUSSION

A system security plan (SSP) is a document that outlines how an organization implements its security requirements. At a minimum, an SSP must include:

- Description of the CMMC Assessment Scope as discussed in **Error! Reference source not found.**;
- CMMC Assessment Scope Description: high-level description of the assets within the assessment scope;
- Description of the Environment of Operation: physical surroundings in which an information system processes, stores, and transmits information;
- Identified and Approved Security Requirements: requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted;
- Implementation Method for Security Requirements: description of how the identified and approved security requirements are implemented with the system or environment;
- Connections and Relationships to Other Systems and Networks: description of related, dependent, and interconnected systems; and
- Defined Frequency of Updates: typically at least annually.

In addition to the requirements above, an SSP often includes:

- general information system description: technical and functional description;
- design philosophies: defense-in-depth strategies and allowed interfaces and network protocols; and

- roles and responsibilities: description of the roles and responsibilities for key personnel, which may include the system owner, system custodian, authorizing officials, and other stakeholders

This practice, CA.L2-3.12.4, which requires developing, documenting, and updating system security plans, promotes effective information security within organizational systems required by SC.L2-3.13.2, as well as other system and communications protection practices.

Example

You are in charge of system security. You develop an SSP and have senior leadership formally approve the document [a]. The SSP explains how your organization handles CUI and defines how that data is stored, transmitted, and protected [d,e]. The criteria outlined in the SSP is used to guide configuration of the network and other information resources to meet your company's goals. Knowing that it is important to keep the SSP current, you establish a policy that requires a formal review and update of the SSP each year [g,h].

Potential Assessment Considerations

- Do mechanisms exist to develop and periodically update an SSP [a,g]?
- Are security requirements identified and approved by the designated authority as non-applicable documented [d]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.12.4

System and Communications Protection (SC)

Level 1 SC Practices

SC.L1-3.13.1 – BOUNDARY PROTECTION

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the external system boundary is defined;

[b] key internal system boundaries are defined;

[c] communications are monitored at the external system boundary;

[d] communications are monitored at key internal boundaries;

[e] communications are controlled at the external system boundary;

[f] communications are controlled at key internal boundaries;

[g] communications are protected at the external system boundary; and

[h] communications are protected at key internal boundaries.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; enterprise security architecture documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers; personnel with boundary protection responsibilities].

Test

[SELECT FROM: Mechanisms implementing boundary protection capability].

DISCUSSION [NIST SP 800-171 R2]

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST SP 800-41 provides guidance on firewalls and firewall policy. NIST SP 800-125B provides guidance on security for virtualization technologies.

FURTHER DISCUSSION

Fences, locks, badges, and key cards help keep non-employees out of your physical facilities. Similarly, your company's IT network or system has boundaries that must be protected. Many companies use a web proxy and a firewall.

When an employee uses a company computer to go to a website, a web proxy makes the request on the user's behalf, looks at the web request, and decides if it should let the employee go to the website.

A firewall controls access from the inside and outside, protecting valuable information and resources stored on the company's network. A firewall stops unwanted traffic on the internet from passing through an outside "fence" to the company's networks and information systems. Internal boundaries determine where data can flow, for instance a software development environment may have its own boundary controlling, monitoring, and protecting the data that can leave that boundary.

You may want to monitor, control, or protect one part of the company network from another. This can also be accomplished with a firewall and limits the ability of attackers and disgruntled employees from entering sensitive parts of your internal network and causing damage.

Example

You are setting up the new network and want to keep your company's information and resources safe. You start by sketching out a simple diagram that identifies the external boundary of your network and any internal boundaries that are needed [a,b]. The first piece of equipment you install is the firewall, a device to separate your internal network from the

internet. The firewall also has a feature that allows you to block access to potentially malicious websites, and you configure that service as well [a,c,e,g]. Some of your coworkers complain that they cannot get onto certain websites [c,e,g]. You explain that the new network blocks websites that are known for spreading malware. The firewall sends you a daily digest of blocked activity so that you can monitor the system for attack trends [c,d].

Potential Assessment Considerations

- What are the external system boundary components that make up the entry and exit points for data flow (e.g., firewalls, gateways, cloud service boundaries), behind which all system components that handle regulated data are contained? What are the supporting system components necessary for the protection of regulated data [a]?
- What are the internal system boundary components that make up the entry and exit points for key internal data flow (e.g., internal firewalls, routers, any devices that can bridge the connection between one segment of the system and another) that separate segments of the internal network – including devices that separate internal network segments such as development and production networks as well as a traditional Demilitarized Zone (DMZ) at the edge of the network [b]?
- Is data flowing in and out of the external and key internal system boundaries monitored (e.g., connections are logged and able to be reviewed, suspicious traffic generates alerts) [c,d]?
- Is data traversing the external and internal system boundaries controlled such that connections are denied by default and only authorized connections are allowed [e,f]?
- Is data flowing in and out of the external and key internal system boundaries protected (e.g., applying encryption when required or prudent, tunneling traffic as needed) [g,h]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.x
- NIST SP 800-171 Rev 2 3.13.1

SC.L1-3.13.5 – PUBLIC-ACCESS SYSTEM SEPARATION

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] publicly accessible system components are identified; and

[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers; personnel with boundary protection responsibilities].

Test

[SELECT FROM: Mechanisms implementing boundary protection capability].

DISCUSSION [NIST SP 800-171 R2]

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies.

NIST SP 800-41 provides guidance on firewalls and firewall policy. SP 800-125B provides guidance on security for virtualization technologies.

FURTHER DISCUSSION

Separate the publicly accessible systems from the internal systems that need to be protected. Do not place internal systems on the same network as the publicly accessible systems and block access by default from DMZ networks to internal networks.

One method of accomplishing this is to create a DMZ network, which enhances security by providing public access to a specific set of resources while preventing connections from those resources to the rest of the IT environment. Some contractors achieve a similar result through the use of a cloud computing environment that is separated from the rest of the company's infrastructure.

Example

The head of recruiting at your company wants to launch a website to post job openings and allow the public to download an application form [a]. After some discussion, your team realizes it needs to use a firewall to create a perimeter network to do this [b]. You host the server separately from the company's internal network and make sure the network on which it resides is isolated with the proper firewall rules [b].

Potential Assessment Considerations

- Are any system components reachable by the public (e.g., internet-facing web servers, VPN gateways, publicly accessible cloud services) [a]?
- Are publicly accessible system components on physically or logically separated subnetworks (e.g., isolated subnetworks using separate, dedicated VLAN segments such as DMZs) [b]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.xi
- NIST SP 800-171 Rev 2 3.13.5

Level 2 SC Practices

SC.L2-3.13.2 – SECURITY ENGINEERING

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] architectural designs that promote effective information security are identified;

[b] software development techniques that promote effective information security are identified;

[c] systems engineering principles that promote effective information security are identified;

[d] identified architectural designs that promote effective information security are employed;

[e] identified software development techniques that promote effective information security are employed; and

[f] identified systems engineering principles that promote effective information security are employed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; system and communications protection policy; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; security architecture documentation; security requirements and specifications for the system; system design documentation; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibility for determining information system security requirements; personnel with information system design, development, implementation, and modification responsibilities; personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan; processes for applying security engineering principles in system specification, design, development, implementation, and modification; automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification].

DISCUSSION [NIST SP 800-171 R2]

Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, 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 developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

NIST SP 800-160-1 provides guidance on systems security engineering.

FURTHER DISCUSSION

Familiarity with security engineering principles and their successful application to your infrastructure will increase the security of your environment. NIST SP 800-160 *System Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* can serve as a source of security engineering and design principles.

Decide which designs and principles to apply. Some will not be possible or appropriate for a given company or for specific systems or components.

Designs and principles should be applied to policies and security standards. Starting with the baseline configuration, they should be extended through all layers of the technology stack (e.g., hardware, software, firmware) and throughout all the components of the infrastructure. The application of these chosen designs and principles should drive you towards a secure architecture with the required security capabilities and intrinsic behaviors present throughout the lifecycle of your technology.

As legacy components age, it may become increasingly difficult for those components to meet security principles and requirements. This should factor into life-cycle decisions for those components (e.g., replacing legacy hardware, upgrading or re-writing software, upgrading run-time environments).

Example

You are responsible for developing strategies to protect data and harden your infrastructure. You are on a team responsible for performing a major upgrade to a legacy system. You refer to your documented security engineering principles [c]. Reviewing each, you decide which are appropriate and applicable [c]. You apply the chosen designs and principles when creating your design for the upgrade [f].

You document the security requirements for the software and hardware changes to ensure the principles are followed. You review the upgrade at critical points in the workflow to ensure the requirements are met. You assist in updating the policies covering the use of the upgraded system so user behavior stays aligned with the principles.

Potential Assessment Considerations

- Does the organization have a defined system architecture [a,d]?
- Are system security engineering principles applied in the specification, design, development and implementation of the systems [d,e,f]?[71]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.2

[71] NIST Handbook 162 Section 3.13.2

SC.L2-3.13.3 – ROLE SEPARATION

Separate user functionality from system management functionality.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] user functionality is identified;

[b] system management functionality is identified; and

[c] user functionality is separated from system management functionality.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Separation of user functionality from system management functionality].

DISCUSSION [NIST SP 800-171 R2]

System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

FURTHER DISCUSSION

Prevent users and user services from accessing system management functionality on IT components (e.g., databases, network components, workstations, servers). This reduces the

attack surface to those critical interfaces by limiting who can access and how they can be accessed. By separating the user functionality from system management functionality, the administrator or privileged functions are not available to the general user.

The intent of this practice is to ensure:

- general users are not permitted to perform system administration functions; and
- system administrators only perform system administration functions from their privileged account.

This can be accomplished using separation like VLANs or logical separation using strong access control methods.

Example

As a system administrator, you are responsible for managing a number of core systems. Policy prevents you from conducting any administration from the computer or system account you use for day-to-day work [a,b]. The servers you manage also are isolated from the main corporate network. To work with them you use a special unique account to connect to a "jump" server that has access to the systems you routinely administer.

Potential Assessment Considerations

- 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) [c]?[72]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.3

[72] NIST Handbook 162 Section 3.13.3

SC.L2-3.13.4 – SHARED RESOURCE CONTROL

Prevent unauthorized and unintended information transfer via shared system resources.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] unauthorized and unintended information transfer via shared system resources is prevented.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Separation of user functionality from system management functionality].

DISCUSSION [NIST SP 800-171 R2]

The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information. This requirement does not address information remnants, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

FURTHER DISCUSSION

No shared system resource, such as cache memory, hard disks, registers, or main memory may pass information from one user to another user. In other words, when objects are reused no residual information should exist on that object. This protects the confidentiality

of the information. This is typically a feature provided by operating system and software vendors.

Example

You are a system administrator responsible for creating and deploying the system hardening procedures for your company's computers. You ensure that the computer baselines include software patches to prevent attackers from exploiting flaws in the processor architecture to read data (e.g., the Meltdown and Spectre exploits). You also verify that the computer operating system is configured to prevent users from accessing other users' folders [a].

Potential Assessment Considerations

- Are shared system resources identified and documented [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.4

SC.L2-3.13.6 – NETWORK COMMUNICATION BY EXCEPTION

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] network communications traffic is denied by default; and

[b] network communications traffic is allowed by exception.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing traffic management at managed interfaces].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

FURTHER DISCUSSION

Block all traffic entering and leaving the network, but permit specific traffic based on organizational policies, exceptions, or criteria. This process of permitting only authorized traffic to the network is called whitelisting and limits the number of unintentional connections to the network.

This practice, SC.L2-3.13.6, requires a deny-all permit by exception approach for all network communications. In doing so, it adds specifics for SC.L1-3.13.1, which only requires monitoring, control, and protection of communication channels.

Example

You are setting up a new environment to house CUI. To properly isolate the CUI network, you install a firewall between it and other networks and set the firewall rules to deny all traffic [a]. You review each service and application that runs in the new environment and determine that you only need to allow http and https traffic outbound [b]. You test the functionality of the required services and make some needed adjustments, then comment each firewall rule so there is documentation of why it is required. You review the firewall rules on a regular basis to make sure no unauthorized changes were made.

Potential Assessment Considerations

- Are network communications traffic on relevant system components (e.g., host and network firewalls, routers, gateways) denied by default (e.g., configured with an implicit deny rule that takes effect in the absence of any other matching traffic rules) [a]?
- Are network communications traffic on relevant system components (e.g., host and network firewalls, routers, gateways) allowed by exception (e.g., configured with explicit allow rules that takes effect only when network traffic matches one or more rules) [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.6

SC.L2-3.13.7 – SPLIT TUNNELING

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms implementing boundary protection capability; mechanisms supporting or restricting non-remote connections].

DISCUSSION [NIST SP 800-171 R2]

Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

FURTHER DISCUSSION

Split tunneling for a remote user utilizes two connections: accessing resources on the internal network via a VPN and simultaneously accessing an external network such as a public network or the internet.

Split tunneling presents a potential opportunity where an open unencrypted connection from a public network could allow an adversary to access resources on internal network. As a mitigation strategy, the split tunneling setting should be disabled on all devices so that all traffic, including traffic for external networks or the internet, goes through the VPN.

Example

You are a system administrator responsible for configuring the network to prevent remote users from using split tunneling. You review the configuration of remote user laptops. You discover that remote users are able to access files, email, database and other services through the VPN connection while also being able to print and access resources on their local network. You change the configuration settings for all company computers to disable split tunneling [a]. You test a laptop that has had the new hardening procedures applied and verify that all traffic from the laptop is now routed through the VPN connection.

Potential Assessment Considerations

- 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 [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.7

SC.L2-3.13.8 – DATA IN TRANSIT

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified;

[b] alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified; and

[c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Cryptographic mechanisms or mechanisms supporting or implementing transmission confidentiality; organizational processes for defining and implementing alternative physical safeguards].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to internal and external networks and any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of the controls for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in commercial telecommunication service packages. If it is infeasible

or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted.

FURTHER DISCUSSION

The intent of this practice is to ensure CUI is cryptographically protected during transit, particularly on the internet. The most common way to accomplish this is to establish a TLS tunnel between the source and destination using the most current version of TLS. This practice does not specify a mutually authenticated handshake, but mutual authentication is the most secure approach to creating a tunnel.

When CMMC requires cryptography, it is to protect the confidentiality of CUI. FIPS-validated cryptography means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. Accordingly, FIPS-validated cryptography is required to meet CMMC practices that protect CUI when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access). 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.

This practice, SC.L2-3.13.8, requires cryptographic mechanisms be used to prevent the disclosure of CUI in-transit and leverages SC.L2-3.13.11, which specifies that the algorithms used must be FIPS-validated.

Example

You are a system administrator responsible for configuring encryption on all devices that contain CUI. Because your users regularly store CUI on laptops and take them out of the office, you encrypt the hard drives with a FIPS-validated encryption tool built into the operating system. For users who need to share CUI, you install a Secure FTP server to allow CUI to be transmitted in a compliant manner [a]. You verify that the server is using a FIPS-validated encryption module by checking the NIST Cryptographic Module Validation Program website [c]. You turn on the "FIPS Compliance" setting for the server during configuration because that is what is required for this product in order to use only FIPS-validated cryptography [c].

Potential Assessment Considerations

- Are cryptographic mechanisms used to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., PDS) [c]?[73]

[73] NIST Handbook 162 Section 3.13.8

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.8

SC.L2-3.13.9 – CONNECTIONS TERMINATION

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a period of inactivity to terminate network connections associated with communications sessions is defined;

[b] network connections associated with communications sessions are terminated at the end of the sessions; and

[c] network connections associated with communications sessions are terminated after the defined period of inactivity.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing network disconnect; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms supporting or implementing network disconnect capability].

DISCUSSION [NIST SP 800-171 R2]

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include de-allocating associated TCP/IP address or 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. Time periods of user inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

FURTHER DISCUSSION

Prevent malicious actors from taking advantage of an open network session or an unattended computer at the end of the connection. Balance user work patterns and needs against security to determine the length of inactivity that will force a termination.

This practice, SC.L2-3.13.9, requires network connections be terminated under certain conditions, which complements AC.L2-3.1.18 that requires control of mobile device connections.

Example

You are an administrator of a server that provides remote access. Your company's policies state that network connections must be terminated after being idle for 60 minutes [a]. You edit the server configuration file and set the timeout to 60 minutes and restart the remote access software [c]. You test the software and verify that the connection is terminated appropriately.

Potential Assessment Considerations

- Are the network connections requiring management and time-out for inactivity documented [a]?
- Are the network connections requiring management and time-out for inactivity configured and implemented [c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.9

SC.L2-3.13.10 – KEY MANAGEMENT

Establish and manage cryptographic keys for cryptography employed in organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] cryptographic keys are established whenever cryptography is employed; and

[b] cryptographic keys are managed whenever cryptography is employed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment and management; system security plan; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for cryptographic key establishment and management].

Test

[SELECT FROM: Mechanisms supporting or implementing cryptographic key establishment and management].

DISCUSSION [NIST SP 800-171 R2]

Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters.

NIST SP 800-56A and NIST SP 800-57-1 provide guidance on cryptographic key management and key establishment.

FURTHER DISCUSSION

Develop processes and technical mechanisms to protect the cryptographic keys' confidentiality, authenticity, and authorized use in accordance with industry standards and regulations. Key management systems provide oversight, assurance, and the capability to demonstrate the cryptographic keys are created in a secure manner and protected from loss or misuse throughout their lifecycle (e.g., active, expired, revoked). For a small number of

keys, this can be accomplished with manual procedures and mechanisms. As the number of keys and cryptographic units increase, automation and tool support will be required.

The first intent of this practice is to ensure cryptographic keys are properly created in a secure manner that prevents them from being reproduced by an adversary. The second intent of this practice is to ensure cryptographic keys are managed in a secure manner that prevents them from being stolen by an adversary.

Key establishment involves the creation of keys and coordination among parties that will use the keys of the methodology for generating the final keying material. This is discussed in detail in SP 800-56A, B, and C.

Key management involves protecting keys when they are distributed, when they are stored, when they are being used, and when they are being recovered.

Key establishment best practices are identified in NIST SP 800-56A, B, and C. Key management best practices are identified in NIST SP 800-57 Parts 1, 2, and 3.

This practice, SC.L2-3.13.10, complements AC.L2-3.1.19 by specifying that any cryptographic keys in use must be protected.

Example 1

You are a system administrator responsible for providing key management. You have generated a public-private key pair to exchange CUI [a]. You require all system administrators to read the key management policy before you allow them to install the private key on their machines [b]. No one else is allowed to know or have a copy of the private key per the policy. You provide the public key to the other parties who will be sending you CUI and test the Public Key Infrastructure (PKI) to ensure the encryption is working [a]. You set a revocation period of one year on all your certificates per organizational policy [b].

Example 2

You encrypt all of your company's computers using the disk encryption utility built into the operating system. As you configure encryption on each device, it generates a cryptographic key. You associate each key with the correct computer in your inventory spreadsheet and restrict access to the spreadsheet to the system administrators whose work role requires them to manage the computers [b].

Potential Assessment Considerations

- Are cryptographic keys established whenever cryptography is employed (e.g., digital signatures, authentication, authorization, transport, or other cryptographic mechanisms) [a]?
- Are cryptographic keys maintained whenever cryptography is employed (e.g., key storage, backup, recovery, revocation, destruction, etc.) [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.10

SC.L2-3.13.11 – CUI ENCRYPTION

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] FIPS-validated cryptography is employed to protect the confidentiality of CUI.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

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

Interview

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

Test

[SELECT FROM: Mechanisms supporting or implementing cryptographic protection].

DISCUSSION [NIST SP 800-171 R2]

Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, 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. Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography.

FURTHER DISCUSSION

When CMMC requires cryptography, it is to protect the confidentiality of CUI. FIPS-validated cryptography means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. Accordingly, FIPS-validated cryptography is required to meet CMMC practices that protect CUI when transmitted or stored outside the protected

environment of the covered contractor information system (including wireless/remote access). 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.

This practice, SC.L2-3.13.11, complements AC.L2-3.1.19, MP.L2-3.8.6, SC.L2-3.13.8, and SC.L2-3.13.16 by specifying that FIPS-validated cryptography must be used.

Example

You are a system administrator responsible for deploying encryption on all devices that contain CUI. You must ensure that the encryption you use on the devices is FIPS-validated cryptography [a]. An employee informs you of a need to carry a large volume of CUI offsite and asks for guidance on how to do so. You provide the user with disk encryption software that you have verified via the NIST website that uses a CMVP-validated encryption module [a]. Once the encryption software is active, the user copies the CUI data onto the drive for transport.

Potential Assessment Considerations

- Is cryptography implemented to protect the confidentiality of CUI at rest and in transit, through the configuration of systems and applications or through the use of encryption tools [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.11

SC.L2-3.13.12 – COLLABORATIVE DEVICE CONTROL

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] collaborative computing devices are identified;

[b] collaborative computing devices provide indication to users of devices in use; and

[c] remote activation of collaborative computing devices is prohibited.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for managing collaborative computing devices].

Test

[SELECT FROM: Mechanisms supporting or implementing management of remote activation of collaborative computing devices; mechanisms providing an indication of use of collaborative computing devices].

DISCUSSION [NIST SP 800-171 R2]

Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

FURTHER DISCUSSION

Notification that a device is in use can include an indicator light that turns on or a specific text window that appears on screen. If a device does not have the means to alert a user when

in use, the organization should provide manual means. Manual means can include, as necessary:

- paper notification on entryways; and
- locking entryways when a collaborative computing device is in use.

This practice is not intended to include technologies that enable users to share the contents of their computer screens via the internet.

Example

A group of remote employees at your company routinely collaborate using cameras and microphones attached to their computers [a]. To prevent the misuse of these devices, you disable the ability to turn on cameras or microphones remotely [c]. You ensure the machines alert users when the camera or microphone are in use with a light beside the camera and an onscreen notification [b]. Although remote activation is blocked, this enables users to see if the devices are active.

Potential Assessment Considerations

- Are the collaborative computing devices configured to provide indication to users when in use (e.g., a light, text notification, or audio tone) or are users alerted before entering a space (e.g., written notice posted outside the space) where they are in use [b]?
- Are the collaborative computing devices configured to prevent them from being turned on without user interaction or consent [c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.12

SC.L2-3.13.13 – MOBILE CODE

Control and monitor the use of mobile code.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] use of mobile code is controlled; and

[b] use of mobile code is monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; system audit logs and records; system security plan; list of acceptable mobile code and mobile code technologies; list of unacceptable mobile code and mobile technologies; authorization records; system monitoring records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing mobile code].

Test

[SELECT FROM: Organizational process for controlling, authorizing, monitoring, and restricting mobile code; mechanisms supporting or implementing the management of mobile code; mechanisms supporting or implementing the monitoring of mobile code].

DISCUSSION [NIST SP 800-171 R2]

Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source.

FURTHER DISCUSSION

Ensure mobile code is authorized to execute in company systems only in accordance with policy and technical configuration, and that unauthorized mobile code is not. Monitor the use of mobile code through boundary devices (e.g., firewalls), audit logs, or security utilities (e.g., mobile device management, advanced endpoint protection) and implement remediation activities as needed.

The first intent of this practice is to ensure the limits of mobile code usage and usage restrictions are documented and enforced. This includes documenting all authorizations for the use of mobile code and ensuring it is not used in other ways. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices to include all mobile devices and smart phones.

The second intent is to monitor the use of mobile code and implement remediation steps if its use does not align with policy.

Example

Your company has decided to prohibit the use of Flash, ActiveX, and Java plug-ins for web browsers on all of its computers [a]. To enforce this policy you configure the computer baseline configuration to disable and deny the execution of mobile code [a]. You implement an exception process to re-enable mobile code execution only for those users with a legitimate business need [a].

One department complains that a web application they need to perform their job no longer works. You meet with them and verify that the web application uses ActiveX in the browser. You submit a change request with the Change Review Board. Once the change is approved, you reconfigure the department's computers to allow the running of ActiveX in the browser. You also configure the company firewall to alert you if ActiveX is used by any website but the allowed one [b]. You set a reminder for yourself to check in with the department at the end of the year to verify they still need that web application.

Potential Assessment Considerations

- Are there defined limits of mobile code usage and established usage restrictions, which specifically authorize use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript) within the information system [a]?[74]
- Is the use of mobile code documented, monitored, and managed (e.g., Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript) [b]?[75]

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.13

[74] NIST Handbook 162 Section 3.13.13
[75] NIST Handbook 162 Section 3.13.13

SC.L2-3.13.14 – VOICE OVER INTERNET PROTOCOL

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] use of Voice over Internet Protocol (VoIP) technologies is controlled; and

[b] use of Voice over Internet Protocol (VoIP) technologies is monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; VoIP implementation guidance; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; system monitoring records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing VoIP].

Test

[SELECT FROM: Organizational process for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP].

DISCUSSION [NIST SP 800-171 R2]

VoIP has different requirements, features, functionality, availability, and service limitations when compared with the Plain Old Telephone Service (POTS) (i.e., the standard telephone service). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

NIST SP 800-58 provides guidance on Voice Over IP Systems.

FURTHER DISCUSSION

Controlling VoIP technologies starts with establishing guidelines and enforcing the appropriate usage that is described in organizational policies. Monitoring should include the users' activity for anything other than what is permitted and authorized and detection of insecure or unauthorized use of the VoIP technology. Security concerns for VoIP include eavesdropping on calls and using ID spoofing to impersonate trusted individuals.

Selecting a solution that can encrypt VoIP traffic is helpful in maintaining the confidentiality and integrity of the voice data.

Example

You are a system administrator responsible for the VoIP system. You configure VoIP for new users after being notified that they have signed the Acceptable Use Policy for VoIP technology [a]. You verify that the VoIP solution is configured to use encryption and have enabled requirements for passwords on voice mailboxes and on phone extension management. You require phone system administrators to log in using multifactor authentication when managing the system [a]. You add the VoIP software to the list of applications that are patched monthly as needed [a,b]. Finally, you configure the VoIP system to send logs to your log aggregator so that they can be correlated with those from other systems and examined for signs of suspicious activity [b].

Potential Assessment Considerations

- Are VoIP technologies (e.g., approved and managed products or solutions) that may or may not be used in the system defined [a]?
- Is monitoring for unapproved VoIP technologies or unapproved use of the allowed VoIP solutions employed [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.14

SC.L2-3.13.15 – COMMUNICATIONS AUTHENTICITY

Protect the authenticity of communications sessions.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the authenticity of communications sessions is protected.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

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

Test

[SELECT FROM: Mechanisms supporting or implementing session authenticity]

DISCUSSION [NIST SP 800-171 R2]

Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. 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.

NIST SP 800-77, NIST SP 800-95, and NIST SP 800-113 provide guidance on secure communications sessions.

FURTHER DISCUSSION

The intent of this practice is to ensure a trust relationship is established between both ends of a communication session. Each end can be assured that the other end is who it is supposed to be. This is often implemented using a mutual authentication handshake when the session is established, especially between devices. Session authenticity is usually provided by a security protocol enforced for a communication session. Choosing and enforcing a protocol will provide authenticity throughout a communications session.

Example

You are a system administrator responsible for ensuring that the two-factor user authentication mechanism for the servers is configured correctly. You purchase and maintain the digital certificate and replace it with a new one before the old one expires. You ensure the TLS configuration settings on the web servers, VPN solution, and other components that use TLS are correct, using secure settings that address risks against attacks on the encrypted sessions [a].

Potential Assessment Considerations

- Is a communications protocol used that ensures the sending and receiving parties do not change during a communications session [a]?
- Are controls in place to validate the identities and information transmitted to protect against man-in-the-middle attacks, session hijacking, and insertion of false information into communications sessions [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.15

SC.L2-3.13.16 – DATA AT REST

Protect the confidentiality of CUI at rest.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the confidentiality of CUI at rest is protected.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

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

Interview

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

Test

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

DISCUSSION [NIST SP 800-171 R2]

Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest.

FURTHER DISCUSSION

CUI at rest means information that is not moving through the network; typically this means data currently stored on hard drives, media, and mobile devices. Implement the necessary security controls to protect the confidentiality of CUI at rest. Although an approved encryption method protects data stored at rest, there are other technical and physical solutions. The methods chosen should depend on the environment and business needs.

Implementing encryption for CUI is one approach to this practice, but it is not mandatory. Physical security is often employed to restrict access to CUI, particularly when it resides on servers within a company's offices. Other approaches for protecting CUI include system-related protections such as configurations and rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content that eliminate attempts at exfiltration. You may also employ other security requirements including secure off-line storage.

This practice, SC.L2-3.13.16, requires confidentially be provided for CUI at rest and complements MP.L2-3.8.9, which requires confidentially of CUI at backup storage locations. This practice, SC.L2-3.13.16, also leverages SC.L2-3.13.11, which specifies that the algorithms used must be FIPS-validated.

Example 1

Your company has a policy stating CUI must be protected at rest and you work to enforce that policy. You research Full Disk Encryption (FDE) products that meet the FIPS encryption requirement. After testing, you deploy the encryption to all computers to protect CUI at rest [a].

Example 2

You have used encryption to protect the CUI on most of the computers at your company, but you have some devices that do not support encryption. You create a policy requiring these devices to be signed out when needed, stay in possession of the signer when checked out, and to be signed back in and locked up in a secured closet when the user is done with the device [a]. At the end of the day each Friday, you audit the sign-out sheet and make sure all devices are returned to the closet.

Potential Assessment Considerations

- Is the confidentiality of CUI at rest protected using encryption of storage devices and/or appropriate physical methods [a]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.13.16

System and Information Integrity (SI)

Level 1 SI Practices

SI.L1-3.14.1 – FLAW REMEDIATION

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the time within which to identify system flaws is specified;

[b] system flaws are identified within the specified time frame;

[c] the time within which to report system flaws is specified;

[d] system flaws are reported within the specified time frame;

[e] the time within which to correct system flaws is specified; and

[f] system flaws are corrected within the specified time frame.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility].

Test

[SELECT FROM: Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms

supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates].

DISCUSSION [NIST SP 800-171 R2]

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including 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 of remediation. NIST SP 800-40 provides guidance on patch management technologies.

FURTHER DISCUSSION

All software and firmware have potential flaws. Many vendors work to remedy those flaws by releasing vulnerability information and updates to their software and firmware. Contractors must have a process to review relevant vendor notifications and updates about problems or weaknesses. After reviewing the information, the contractor must implement a patch management process that allows for software and firmware flaws to be fixed without adversely affecting the system functionality. Contractors must define the time frames within which flaws are identified, reported, and corrected for all systems. Contractors should consider purchasing support from their vendors to ensure timely access to updates.

Example

You know that software vendors typically release patches, service packs, hot fixes, etc. and want to make sure your software is up to date. You develop a policy that requires checking vendor websites for flaw notifications every week [a]. The policy further requires that those flaws be assessed for severity and patched on end-user computers once each week and servers once each month [c,e]. Consistent with that policy, you configure the system to check for updates weekly or daily depending on the criticality of the software [b,e]. Your team reviews available updates and implements the applicable ones according to the defined schedule [f].

Potential Assessment Considerations

- Is the time frame (e.g., a set number of days) within which system flaw identification activities (e.g., vulnerability scans, configuration scans, manual review) must be performed defined and documented [a]?

- Are system flaws (e.g., vulnerabilities, misconfigurations) identified in accordance with the specified time frame [b]?
- Is the time frame (e.g., a set number of days dependent on the assessed severity of a flaw) within which system flaws must be corrected defined and documented [e]?
- Are system flaws (e.g., applied security patches, made configuration changes, or implemented workarounds or mitigations) corrected in accordance with the specified time frame [f]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.xii
- NIST SP 800-171 Rev 2 3.14.1

SI.L1-3.14.2 – MALICIOUS CODE PROTECTION

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] designated locations for malicious code protection are identified; and

[b] protection from malicious code at designated locations is provided.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].

Test

[SELECT FROM: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting or implementing malicious code scanning and subsequent actions].

DISCUSSION [NIST SP 800-171 R2]

Designated locations include system entry and exit points which may include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways

including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of 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 organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations 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 the functions intended. NIST SP 800-83 provides guidance on malware incident prevention.

FURTHER DISCUSSION

A designated location may be a network device such as a firewall or an end user's computer.

Malicious code, which can be delivered by a range of means (e.g., email, removable media, or websites), includes the following:

- virus – program designed to damage, steal information, change data, send email, show messages, or any combination of these things;
- spyware – program designed to gather information about a person's activity in secret when they click on a link, usually installed without the person knowing ;
- trojan horse – type of malware made to look like legitimate software and used by cyber criminals to get access to a company's systems; and
- ransomware – type of malware that threatens to publish the contractor's data or perpetually block access to it unless a ransom is paid.

Use anti-malware tools to stop or lessen the impact of malicious code.

Example

You are buying a new computer and want to protect your company's information from viruses, spyware, etc. You buy and install anti-malware software [a,b].

Potential Assessment Considerations

- Are system components (e.g., workstations, servers, email gateways, mobile devices) for which malicious code protection must be provided identified and documented [a]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.xiii
- NIST SP 800-171 Rev 2 3.14.2

SI.L1-3.14.4 – UPDATE MALICIOUS CODE PROTECTION

Update malicious code protection mechanisms when new releases are available.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] malicious code protection mechanisms are updated when new releases are available.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].

Test

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

DISCUSSION [NIST SP 800-171 R2]

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 organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations 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.

FURTHER DISCUSSION

Malware changes on an hourly or daily basis, and it is important to update detection and protection mechanisms frequently to maintain the effectiveness of the protection.

Example

You have installed anti-malware software to protect a computer from malicious code. Knowing that malware evolves rapidly, you configure the software to automatically check for malware definition updates every day and update as needed [a].

Potential Assessment Considerations

- Is there a defined frequency by which malicious code protection mechanisms must be updated (e.g., frequency of automatic updates or manual processes) [a]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.xiv
- NIST SP 800-171 Rev 2 3.14.4

SI.L1-3.14.5 – SYSTEM & FILE SCANNING

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the frequency for malicious code scans is defined;

[b] malicious code scans are performed with the defined frequency; and

[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].

Test

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

DISCUSSION [NIST SP 800-171 R2]

Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety

of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

FURTHER DISCUSSION

Use anti-malware software to scan for and identify viruses in your computer systems and determine how often scans are conducted. Real-time scans look at the system whenever new files are downloaded, opened, and saved. Periodic scans check previously saved files against updated malware information.

Example

You work with your company's email provider to enable enhanced protections that will scan all attachments to identify and quarantine those that may be harmful prior to a user opening them [c]. In addition, you configure antivirus software on each computer to scan for malicious code every day [a,b]. The software also scans files that are downloaded or copied from removable media such as USB drives. It quarantines any suspicious files and notifies the security team [c].

Potential Assessment Considerations

- Are files from media (e.g., USB drives, CD-ROM) included in the definition of external sources and are they being scanned [c]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.xv
- NIST SP 800-171 Rev 2 3.14.5

Level 2 SI Practices

SI.L2-3.14.3 – SECURITY ALERTS & ADVISORIES

Monitor system security alerts and advisories and take action in response.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] response actions to system security alerts and advisories are identified;

[b] system security alerts and advisories are monitored; and

[c] actions in response to system security alerts and advisories are taken.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; procedures addressing security alerts, advisories, and directives; system security plan; records of security alerts and advisories; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security alert and advisory responsibilities; personnel implementing, operating, maintaining, and using the system; personnel, organizational elements, and external organizations to whom alerts, advisories, and directives are to be disseminated; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; mechanisms supporting or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives; mechanisms supporting or implementing security directives].

DISCUSSION [NIST SP 800-171 R2]

There are many publicly available sources of system security alerts and advisories. The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and relevant industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations,

for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations.

NIST SP 800-161 provides guidance on supply chain risk management.

FURTHER DISCUSSION

Solicit and receive security alerts, advisories, and directives from reputable external organizations. Identify sources relevant to the industry and technology used by your company. Methods to receive alerts and advisories may include:

- signing up for email distributions;
- subscribing to RSS feeds; and
- attending meetings.

Review alerts and advisories for applicability as they are received. The frequency of the reviews should be based on the frequency of the alerts and advisories to ensure you have the most up-to-date information.

External alerts and advisories may prompt you to generate internal security alerts, advisories, or directives, and share these with all personnel with a need-to-know. The individuals should assess the risk related to a given alert and act to respond as appropriate. Sometimes it may require a configuration update. Other times, the information may also require adjusting system architecture in order to thwart a threat described in an advisory.

Example

You monitor security advisories each week. You review the alert emails and online subscription service alerts to determine which ones apply [b]. You create a list of the applicable alerts and research what steps you need to take to address them. Next, you generate a plan that you review with your change management group so that the work can be scheduled [c].

Potential Assessment Considerations

- Are the responses to system security alerts and advisories identified in relation to the assessed severity of potential flaws (e.g., communicating with responsible personnel, initiating vulnerability scans, initiating system flaw remediation activities) [a]?
- Are system security alerts and advisories addressed (e.g., assessing potential severity or likelihood, communicating with responsible personnel, initiating vulnerability scans, initiating system flaw remediation activities) [a,c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.14.3

SI.L2-3.14.6 – MONITOR COMMUNICATIONS FOR ATTACKS

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the system is monitored to detect attacks and indicators of potential attacks;

[b] inbound communications traffic is monitored to detect attacks and indicators of potential attacks; and

[c] outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and information integrity policy; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram or layout; system security plan; system monitoring tools and techniques documentation; system design documentation; locations within system where monitoring devices are deployed; system protocols; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility monitoring the system; personnel with responsibility for the intrusion detection system].

Test

[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing intrusion detection capability and system monitoring; mechanisms supporting or implementing system monitoring capability; organizational processes for intrusion detection and system monitoring; mechanisms supporting or implementing the monitoring of inbound and outbound communications traffic].

DISCUSSION [NIST SP 800-171 R2]

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring

within the system. Organizations can monitor systems, for example, by observing audit record 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. 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 being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of 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.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

NIST SP 800-94 provides guidance on intrusion detection and prevention systems.

FURTHER DISCUSSION

Think of indicators of attack as a set of footprints an adversary leaves during an attack. Indicators of attack provide information on the steps the adversary followed and its intent. Indicators of attacks on organizational systems may include:

- internal traffic that indicates the presence of malicious code;
- anomalous activity detected during non-business hours;
- unauthorized data leaving the organization; and
- communicating to external information systems.

To detect attacks and indicators of attacks, deploy monitoring devices or agents. Place these sensors at strategic points within the systems and networks to collect essential information. Strategic points include internal and external system boundaries. Monitor both inbound traffic and outbound traffic as well as actions on hosts.

This practice, SI.L2-3.14.6, provides details for the communications of organizational systems. SI.L2-3.14.6 supports the practice AU.L2-3.3.1, which involves creating and retaining records for monitoring, analysis, and investigations.

Example

It is your job to look for known indicators of attack or anomalous activity within your systems and communications traffic [a,b,c]. Because these indicators can show up in a variety of places on your network, you have created a checklist of places to check each week. These include the office firewall logs, the audit logs of the file server where CUI is stored, and the connection log for your VPN gateway [b].

You conduct additional reviews when you find an indicator, or something that does not perform as it should [a].

Potential Assessment Considerations

- Are details provided for the methodology of determining attacks and indicators of attack [a]?
- Are monitoring devices deployed within the information system to collect information that may indicate an attack [a]?
- Are communications traffic flows understood and is there a deployed capability to review that traffic [b,c]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.14.6

SI.L2-3.14.7 – IDENTIFY UNAUTHORIZED USE

Identify unauthorized use of organizational systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized use of the system is defined; and

[b] unauthorized use of the system is identified.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram/layout; system security plan; system design documentation; system monitoring tools and techniques documentation; locations within system where monitoring devices are deployed; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for monitoring the system].

Test

[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing system monitoring capability].

DISCUSSION [NIST SP 800-171 R2]

System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring 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). Output from system monitoring serves as input to continuous monitoring and incident response programs.

Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements,

including the need for specific types of system monitoring, may be referenced in other requirements.

NIST SP 800-94 provides guidance on intrusion detection and prevention systems.

FURTHER DISCUSSION

Define authorized use of your systems. Create an acceptable use policy to establish the baseline for how users access devices, internal network services, and the internet. Define authorized use by specific roles such as: user, administrator, and technician. After authorized use is defined, identify unauthorized use of systems.

Monitor systems by observing audit activities from the system logs. This can be accomplished in real time using automated solutions or by manual means. To identify unauthorized use, leverage existing tools and techniques, such as:

- intrusion detection systems;
- intrusion prevention systems;
- malicious code protection software;
- scanning tools;
- audit record monitoring software; and
- network monitoring software.

This practice, SI.L2-3.14.7, which deals with identifying unauthorized use of organizational systems, is related to practices: AC.L1-3.1.1, AU.L2-3.3.1, IA.L1-3.5.1, and IA.L1-3.5.2. All of these practices help create the building blocks that support SI.L2-3.14.7.

Example 1

You are in charge of IT operations. You need to ensure that everyone using an organizational system is authorized to do so and conforms to the written authorized use policy. To do this, you deploy an application that monitors user activity and records the information for later analysis. You review the data from this application for signs of activity that does not conform to the acceptable use policy [a,b].

Example 2

You are alerted through your Intrusion Detection System (IDS) that one of your users is connecting to a server that is from a high-risk domain (based on your commercial domain reputation service). You investigate and determine that it's not the user, but instead an unauthorized connection attempt [b]. You add the domain to your list of blocked domains to prevent connections in the future.

Potential Assessment Considerations

- Is authorized use of systems defined (e.g., data types permitted for storage or processing, personnel authorized to access, times or days of permitted use, permitted software) [a]?

- Is unauthorized use of systems defined (e.g., not authorized to use systems for bitcoin mining, not authorized for pornographic content, not authorized to access gambling games/content) [b]?

KEY REFERENCES

- NIST SP 800-171 Rev 2 3.14.7

Appendix A – Acronyms and Abbreviations

AC	Access Control
AES	Advanced Encryption Standard
API	Application Programming Interface
AT	Awareness and Training
AU	Audit and Accountability
C3PAO	CMMC Third-Party Assessment Organization
CA	Security Assessment
CD-ROM	Compact Disk Read-Only Memory
CIO	Chief Information Officer
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CMVP	Cryptographic Module Validation Program
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DFARS	Defense Federal Acquisition Regulation Supplement
DHC	Device Health Check
DIB	Defense Industrial Base
DMZ	Demilitarized Zone
DoD	Department of Defense
DVD	Digital Versatile Disc or Digital Video Disc
ESP	External Service Provider
FAQ	Frequently Asked Question
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCI	Federal Contract Information
FDDI	Fiber Distributed Data Interface
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
IA	Identification and Authentication
ID	Identification

IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
ISAC	Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network
IT	Information Technology
LAN	Local Area Network
MA	Maintenance
MAC	Media Access Control
MDM	Mobile Device Management
MEP	Manufacturing Extension Partnership
MFA	Multifactor Authentication
MP	Media Protection
NARA	National Archives and Records Administration
NAS	Networked Attached Storage
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OS	Operating System
OT	Operational Technology
PDA	Personal Digital Assistant
PE	Physical Protection
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
PS	Personnel Security
RADIUS	Remote Authentication Dial-in User Service
RA	Risk Assessment
SC	System and Communications Protection
SI	System and Information Integrity
SMS	Short Message Service

SOC	Security Operations Center
SP	Special Publication
SSP	System Security Plan
TLS	Transport Layer Security
URL	Universal Resource Locator (aka Uniform Resource Locator)
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUENCODE	Unix-to-Unix Encode
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WPA2-PSK	WiFi Protected Access-Pre-shared Key

This page intentionally left blank.


OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT
CYBERSECURITY MATURITY MODEL
CERTIFICATION