CMMC Self-Assessment Guide

Level 1

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

Introduction

This document provides self-assessment guidance for Level 1 of the Cybersecurity Maturity Model Certification (CMMC). Guidance for conducting a CMMC Level 2 assessment can be found in *CMMC Assessment Guide – Level 2*. Guidance for conducting a CMMC Level 3 assessment will be published at a later date as the *CMMC Assessment Guide – Level 3* document. More details on the CMMC Model can be found in the *CMMC Model Overview* document.

CMMC Level 1 focuses on the protection of Federal Contract Information (FCI), which is defined as follows:

> *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 1 encompasses the basic safeguarding requirements specified in Federal Acquisition Regulation (FAR) Clause 52.204-21.

Purpose and Audience

This guide is intended for contractors that will be conducting a CMMC Level 1 self-assessment and the professionals or companies that will support them in those efforts.

Document Organization

This document is organized into the following sections:

- **Self-Assessment and Compliance:** Provides an overview of the CMMC self-assessment process, how to document compliance, guidance around contractor size, and self-assessment scope information.
- **Self-Assessment Criteria and Methodology:** Provides guidance on the criteria and methodology (i.e., *interview*, *examine*, and *test*) to be employed during a CMMC self-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 self-assessment requirements and specifics for each CMMC practice.

Self-Assessment and Compliance

An annual Level 1 self-assessment, with an accompanying senior company official affirmation of compliance in the Supplier Performance Risk System (SPRS)[1], asserts that a contractor is meeting all the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21. Contractors should use the self-assessment methods as defined in this guide. Once a contractor has self-assessed and finds they are in compliance with Level 1 practices, other entities (e.g., government sponsors and prime contractors looking to hire subcontractors) have increased confidence that the contractor meets CMMC Level 1 practices.

A contractor can be in compliance with CMMC Level 1 practices for an entire enterprise network or for particular enclave(s), depending upon where the FCI is or will be processed, stored, or transmitted.

Contactors can choose to perform the annual self-assessment internally or engage a third-party to assist with evaluating their Level 1 compliance. Use of a third-party to assist is still considered a self-assessment and does not result in a certification.

Contractor Size

The CMMC self-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.

Self-Assessment Scope

Prior to conducting a CMMC self-assessment, the contractor must specify the CMMC Self-Assessment Scope. The CMMC Self-Assessment Scope identifies which assets within the contractor's environment will be assessed and the details of the self-assessment. For a CMMC Level 1 self-assessment, the assets that process, store, or transmit FCI are considered in-scope and should be assessed against the CMMC Level 1 practices. See the *CMMC Self-Assessment Scope – Level 1* document for additional information.

[1] For more information go to: https://www.sprs.csd.disa.mil/

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 National Institute of Standards and Technology (NIST) documentation, it is important to understand 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 Level 1 practices presented later in the document.

The specific terms associated with CMMC Level 1 are:

- **Asset (Organizational Asset):** Anything that has value to an organization, including, but not limited to: another organization, person, computing device, information technology (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 Self-Assessment Scope; for more information, see *CMMC Self-Assessment Scope – Level 1*.
- **Component:** A discrete identifiable information technology *asset* that represents a building block of a system and may include hardware, software, and firmware [NIST SP 800-171 Rev 2 under system component NIST SP 800-128]. A *component* is one type of *asset*.
- **Information System (IS):** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [NIST 800-171 Rev 2]. An *IS* is one type of *asset*.
- **Monitor:** The act of continual 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].

Assessment Criteria and Methodology

The *CMMC Self-Assessment Guide – Level 1* leverages the assessment procedure described in NIST Special Publication (SP) 800-171A Section 2.1[2] as modified below in brackets:

> *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 practice produces assessment findings. These findings reflect, or are subsequently used, to help determine if the 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, and 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* ***[Self-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.*

[2] NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*, June 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 800-171A focuses on Controlled Unclassified Information (CUI). Since CMMC Level 1 focuses on safeguarding FCI, the applicable self-assessment objectives for Level 1 are updated to address FCI in lieu of CUI.

Criteria

Self-assessment objectives are provided for each Level 1 practice and are based on existing criteria (i.e., NIST SP 800-171A) modified for FCI in lieu of CUI. The criteria are authoritative and provide a basis to conduct a self-assessment of a practice.

Methodology

The primary result of a self-assessment is a self-assessment report, which contains the findings associated with the self-assessment.

To verify and validate that a contractor is meeting CMMC practices, evidence needs to exist demonstrating that the contractor has fulfilled the objectives of the Level 1 practices. Because different self-assessment objectives can be met in different ways (e.g., through documentation, computer configuration, network configuration, or training) a variety of techniques may be used, including any of the three assessment methods described above from NIST SP 800-171A, to determine if the contractor meets the intent of the Level 1 practices.

Follow the guidance in NIST SP 800-171A when determining which self-assessment methods to use:

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

For more detailed information on assessment methods, see NIST SP 800-171A Appendix D.

Who Is Interviewed

Interviews of applicable staff (possibly at different organizational levels) determine if Level 1 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, review documentation to determine if assessment objectives are met. Interviews with staff may identify the documents the contractor uses. Documents need to be in their final forms; drafts of policies or documentation are not eligible to be used 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 applicable:

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system, 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 for evidence of compliance.

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

What Is Tested

Testing is an important part of the self-assessment process. Interviews tell 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. Not all practices will require testing.

Practice Findings

The self-assessment of a CMMC practice results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE. To demonstrate CMMC Level 1 compliance, the contractor will need a finding of MET or NOT APPLICABLE on all Level 1 practices.

- **MET**: The contractor successfully meets the practice. For each practice marked MET, include statements that indicate the response conforms to all objectives and document the appropriate evidence to support the response.
- **NOT MET**: The contractor has not met the practice. For each practice marked NOT MET, include statements that explain why and document the appropriate evidence showing that the contractor does not conform fully to all of the objectives.
- **NOT APPLICABLE (N/A)**: The practice does not apply for the self-assessment. For each practice marked N/A, include 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 because 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, or 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, include 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

Introduction

This section provides detailed information for how to self-assess each CMMC practice. The section is organized by domain and then practices. 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 [NIST SP 800-171A]:** Identifies the specific set of objectives that must be met to receive MET for the practice as defined in NIST SP 800-171A.
- **Potential Assessment Methods and Objects [NIST SP 800-171A]:** Defines the nature and the extent of the self-assessment actions as defined in NIST SP 800-171A. The methods include *examine*, *interview*, and *test*. Self-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 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.
    - Provides potential assessment considerations. These may include common considerations for assessing the practice and potential questions that may be asked when assessing the objectives, including, in some cases, questions from NIST Handbook 162[3].
- **Key References:** Lists the related basic safeguarding requirement from FAR Clause 52.204-21 and the security requirement from NIST SP 800-171 Rev 2. The *CMMC Model Overview, Appendix B: Source Mapping* provides additional references.

[3] 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)

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]?[4]

[4] NIST Handbook 162 Section 3.1.1

KEY REFERENCES

- FAR Clause 52.204-21 b.1.i
- NIST SP 800-171 Rev 2 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]?[5]
- 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]?[6]

KEY REFERENCES

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

[5] NIST Handbook 162 Section 3.1.2
[6] 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 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 (e.g., 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

Identification and Authentication (IA)

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

Media Protection (MP)

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]?[7]

KEY REFERENCES

- FAR Clause 52.204-21 b.1.vii
- NIST SP 800-171 Rev 2 3.8.3

[7] NIST Handbook 162 Section 3.8.3

Physical Protection (PE)

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]?[8]
- 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]?[9]
- Are output devices such as printers placed in areas where their use does not expose data to unauthorized individuals [c]?[10]

KEY REFERENCES

- FAR Clause 52.204-21 b.1.viii
- NIST SP 800-171 Rev 2 3.10.1

[8] NIST Handbook 162 Section 3.10.1
[9] NIST Handbook 162 Section 3.10.1
[10] 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 Personal Identity Verification (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]?[11]
- Are visitor access records retained for as long as required [a]?[12]

KEY REFERENCES

- FAR Clause 52.204-21 Partial b.1.ix
- NIST SP 800-171 Rev 2 3.10.4

[11] NIST Handbook 162 Section 3.10.4
[12] 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

System and Communications Protection (SC)

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 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 firm 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

System and Information Integrity (SI)

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 PROECTION

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

Malicious code purposely performs unauthorized activity that undermines the security of an information system. 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, usually installed without the person knowing when they click on a link;
- 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 and spyware. 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 than the functions intended.

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 and 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

Appendix A – Acronyms and Abbreviations

AC	Access Control
CD-ROM	Compact Disk Read-Only Memory
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DFARS	Defense Federal Acquisition Regulation Supplement
DMZ	Demilitarized Zone
DoD	Department of Defense
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
ID	Identification
IT	Information Technology
LAN	Local Area Network
MEP	Manufacturing Extension Partnership
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
SC	System and Communications Protection
SI	System and Information Integrity
SP	Special Publication
SPRS	Supplier Performance Risk System
USB	Universal Serial Bus
UUENCODE	Unix-to-Unix Encode
VLAN	Virtual Local Area Network


OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT
CYBERSECURITY MATURITY MODEL
CERTIFICATION