CMMC Assessment Guide
Level 1

Version – 2.13 | September 2024
DoD-CIO-00002 (ZRIN 0790-ZA18)

24-T-2764

NOTICES

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or departmental policies.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

TABLE OF CONTENTS

Introduction **1**

Assessment and Compliance **2**

Assessment Scope 2

CMMC-Custom Terms **3**

Assessment Criteria and Methodology **5**

Criteria 6

Methodology 6

Assessment Findings 8

Requirement Descriptions **10**

Introduction 10

Access Control (AC) **12**

AC.L1-b.1.i – Authorized Access Control [FCI Data] 12

AC.L1-b.1.ii – Transaction & Function Control [FCI Data] 15

AC.L1-b.1.iii – External Connections [FCI Data] 17

AC.L1-b.1.iv – Control Public Information [FCI Data] 20

Identification and Authentication (IA) **22**

IA.L1-b.1.v – Identification [FCI Data] 22

IA.L1-b.1.vi – Authentication [FCI Data] 24

Media Protection (MP) **27**

MP.L1-b.1.vii – Media Disposal [FCI Data] 27

Physical Protection (PE) **29**

PE.L1-b.1.viii – Limit Physical Access [FCI Data] 29

PE.L1-b.1.ix – Manage Visitors & Physical Access [FCI Data] 31

System and Communications Protection (SC) **34**

SC.L1-b.1.x – Boundary Protection [FCI Data] 34

SC.L1-b.1.xi – Public-Access System Separation [FCI Data] 37

System and Information Integrity (SI) **39**

SI.L1-b.1.xii – Flaw Remediation [FCI Data] 39

SI.L1-b.1.xiii – Malicious Code ProTection [FCI Data] 42

SI.L1-b.1.xiv – Update Malicious Code Protection [FCI Data] 45
SI.L1-b.1.xv – System & File Scanning [FCI Data] 47

Appendix A – Acronyms and Abbreviations 49

Introduction

This document provides guidance in the preparation for and execution of a Level 1 self-assessment under the Cybersecurity Maturity Model Certification (CMMC) Program as set forth in section 170.15 of title 32, Code of Federal Regulations (CFR). Guidance for conducting a Level 2 self-assessment or certification assessment can be found in *CMMC Assessment Guide – Level 2*. Guidance for conducting a Level 3 certification assessment can be found in *CMMC Assessment Guide – Level 3*. More details on the CMMC Model can be found in *CMMC Model Overview*.

Level 1 focuses on the protection of Federal Contract Information (FCI), which is defined in 32 CFR § 170.4 and 48 CFR § 4.1901:

> *Federal contract information means 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.*

Level 1 is comprised of the 15 basic safeguarding requirements specified in Federal Acquisition Regulation (FAR) Clause 52.204-21.

Purpose and Audience

This guide is intended for Organizations Seeking Assessment (OSAs), cybersecurity professionals, and individuals and companies that support CMMC efforts. This document can be used as part of preparation for and conducting a Level 1 self-assessment.

Document Organization

This document is organized into the following sections:

- **Assessment and Compliance:** provides an overview of the Level 1 self-assessment process set forth in 32 CFR § 170.15, describes ways of documenting compliance, and provides guidance regarding OSA size and the self-assessment scope requirements set forth in 32 CFR § 170.19.
- **CMMC-Custom Terms:** incorporates definitions from 32 CFR § 170.4 and definitions included by reference from 32 CFR § 170.2, and provides clarification of the intent and scope of custom terms as used in the context of CMMC.
- **Assessment Criteria and Methodology:** provides guidance on criteria and methodology (i.e., *interview*, *examine*, and *test*) that may be employed during a Level 1 self-assessment, as well as on assessment findings.
- **Requirement Descriptions:** provides guidance specific to each Level 1 security requirement.

Assessment and Compliance

Level 1 self-assessment requirements are set forth in 32 CFR § 170.15. The OSA will assess its own contractor information system(s) to determine if it meet all the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21. OSAs should use the self-assessment methods as described in 32 CFR § 170.15.

Level 1 requirements may apply to an entire enterprise infrastructure or to a particular enclave(s), depending upon where the FCI will be processed, stored, or transmitted.

OSAs can choose to perform the annual self-assessment internally or engage a third party to assist. Use of a third party to assist is still considered a self-assessment and does not result in a certification. The primary result of a self-assessment is the submission of Level 1 compliance results into the Supplier Performance Risk System (SPRS) and a self-assessment report, which contains the findings associated with the self- assessment.

Assessment Scope

Prior to conducting a Level 1 self-assessment, the OSA must specify the CMMC Assessment Scope as defined in 32 CFR § 170.19(a). The CMMC Assessment Scope identifies which assets within the OSA's environment will be assessed and the details of the self-assessment. In accordance with §170.19, for a Level 1 self-assessment, the assets that process, store, or transmit FCI are considered in-scope and should be assessed against the Level 1 requirements. See the *CMMC Scoping Guide – Level 1* document for additional information.

CMMC-Custom Terms

The CMMC Program has custom terms that align with program requirements. Although some terms may have other definitions in open forums, it is important to understand these terms as they apply to the CMMC Program.

The custom terms associated with Level 1 are:

- **Assessment:** As defined in 32 CFR § 170.4 means 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, as defined in 32 CFR § 170.15 to 32 CFR § 170.18.
    - Level 1 self-assessment is the term for the activity performed by an OSA to evaluate its own information system, when seeking a CMMC Status of Final Level 1 (Self).
- **Assessment Objective:** A set of determination statements that, taken together, expresses the desired outcome for the assessment of a security requirement. Successful implementation of the corresponding CMMC security requirement requires meeting all applicable assessment objectives defined in NIST SP 800–171A or NIST SP 800-172A.
- **Asset:** An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns, as defined in NIST SP 800-160 Rev 1.
- **CMMC Status:** As defined in 32 CFR § 170.4 is the result of meeting or exceeding the minimum required score for the corresponding assessment. The CMMC Status of an OSA information system is officially stored in SPRS and additionally presented on a Certificate of CMMC Status, if the assessment was conducted by a C3PAO or DCMA DIBCAC.
    - Final Level 1 (Self) is defined in § 170.15(c)(1). To achieve a CMMC Status of Final Level 1 (Self) the OSA must conduct a Level 1 self-assessment scored in accordance with the CMMC Scoring Methodology described in § 170.24. The Level 1 self-assessment must be performed in accordance with the Level 1 scope requirements set forth in § 170.19(a) and (b). In instances where an objective addresses CUI, the term FCI should be substituted for CUI.
- **Component:** A discrete identifiable information technology *asset* that represents a building block of a system and may include hardware, software, and firmware[1]. A *component* is one type of *asset*.

[1] NIST SP 800-171 Rev 2, p 59 under system component

- **Enduring Exception:** A special circumstance or system where remediation and full compliance with CMMC security requirements is not feasible. Examples include systems required to replicate the configuration of 'fielded' systems, medical devices, test equipment, OT, and IoT. No operational plan of action is required but the circumstance must be documented within a system security plan. Specialized Assets and GFE may be Enduring Exceptions.
- **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*.
- **Monitoring:** Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected [NIST SP 800-160 Vol 1].
- **Operational plan of action:** As used in security requirement CA.L2-3.12.2, means the formal artifact which identifies temporary vulnerabilities and temporary deficiencies in implementation of requirements and documents how and when they will be mitigated, corrected, or eliminated. The OSA defines the format (e.g., document, spreadsheet, database) and specific content of its operational plan of action. An operational plan of action is not the same as a POA&M associated with an assessment.
- **Organization-Defined:** As determined by the OSA being assessed except as defined in the case of Organization-Defined Parameter (ODP). 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 an OSA's solution.
- **Temporary deficiency:** As defined in 32 CFR § 170.4 means a condition where remediation of a discovered deficiency is feasible and a known fix is available or is in process. The deficiency must be documented in an operational plan of action. A temporary deficiency is not based on an 'in progress' initial implementation of a CMMC security requirement but arises after implementation. A temporary deficiency may apply during the initial implementation of a security requirement if, during roll-out, specific issues with a very limited subset of equipment is discovered that must be separately addressed. There is no standard duration for which a temporary deficiency may be active. For example, FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency.

Assessment Criteria and Methodology

This *CMMC Assessment Guide – Level 1* provides guidance regarding the assessment procedures required by 32 CFR § 170.15, which requires the Level 1 self-assessment to be performed using the objectives defined in NIST Special Publication (SP) 800-171A[2]. NIST SP 800-171A Section 2.1 says the following:

> *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 requirement that is the subject of the assessment. The determination statements are linked to the content of the requirement to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to a requirement produces assessment findings. These findings reflect, or are subsequently used, to help determine if the requirement has been satisfied.*
>
> *Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals.*
>
> - *Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, 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 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.*

[2] NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information,* June 2018 (italics and bulleted list formatting altered)

- *And finally, the* test *method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior.*

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

The guidance specified in NIST SP 800-171A focuses on Controlled Unclassified Information (CUI). Since Level 1 focuses on safeguarding FCI, the applicable self-assessment objectives for Level 1 are modified to address FCI rather than CUI as set forth in 32 CFR § 170.15(c)(1)(i). Where **CUI** is noted in a NIST SP 800-171A assessment objective, **[FCI]** has been substituted in the Level 1 objective description. Level 1 security requirement descriptions align with FAR Clause 52.204-21.

Criteria

Assessment objectives are provided for each Level 1 requirement and are based on existing criteria in NIST SP 800-171A modified for FCI rather than CUI as set forth in 32 CFR § 170.15(c)(1)(i). The criteria are authoritative and provide the basis for the self-assessment of a requirement.

Methodology

To verify and validate that an OSA is meeting CMMC requirements, evidence needs to exist demonstrating that the OSA has fulfilled the objectives of the Level 1 requirements. 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 to determine if the OSA meets the Level 1 requirements, including any of the three assessment methods from NIST SP 800-171A.

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

Organizations [OSAs] are not expected to employ all assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the [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) may provide information to help an entity determine if Level 1 security requirements have been implemented, as well as if adequate resourcing, training, and planning have occurred for individuals to implement the security requirements.

What Is Examined

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

For some security requirements, review of documentation may assist an entity in determining if the assessment objectives have been met. Interviews with staff may help identify relevant documents. As set forth in 32 CFR § 170.24, 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 still subject to change. Common types of documents that may be used as evidence include:

- 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. An OSA may not have these specific documents, and other documents may be reviewed.

In other cases, the security requirement 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 provide information about what the OSA staff believe to be true, documentation provides evidence of implementing policies and procedures, and testing demonstrates what has or has not been done. For example, OSA 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 requirement is met. Not all security requirements utilize testing to allow an entity to determine if whether the assessment objective has been met.

Assessment Findings

The self-assessment of a CMMC requirement results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE as defined in 32 CFR § 170.24. To demonstrate Level 1 compliance, the OSA will need a finding of MET or NOT APPLICABLE on all Level 1 security requirements.

- **MET**: All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include working papers, drafts, and unofficial or unapproved policies. For each security requirement marked MET, it is best practice to record statements that indicate the response conforms to all objectives and document the appropriate evidence to support the response.
    - Enduring Exceptions when described, along with any mitigations, in the system security plan shall be assessed as MET.
    - Temporary deficiencies that are appropriately addressed in operational plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) shall be assessed as MET.
- **NOT MET**: One or more objectives of the security requirement is not satisfied. For each security requirement marked NOT MET, it is best practice to record statements that explain why and document the appropriate evidence showing that the OSA does not conform fully to all of the objectives.
- **NOT APPLICABLE (N/A)**: A security requirement and/or objective do not apply at the time of the assessment. For each security requirement marked N/A, it is best practice to record a statement that explains why the requirement does not apply to the OSA. For example, SC.L1-b.1.xi might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope. During an assessment, an assessment objective assessed as N/A is equivalent to the same assessment objective being assessed as MET.

  Each assessment objective in NIST SP 800-171A must yield a finding of MET or NOT APPLICABLE in order for the overall security requirement to be scored as MET. Assessors exercise judgment in determining when sufficient and adequate evidence has been presented to make an assessment finding.

  CMMC assessments are conducted and results are captured at the assessment objective level. One NOT MET Assessment Objective results in a failure of the entire security requirement.

  A security requirement can be applicable even when assessment objectives included in the security requirement are scored N/A. The security requirement is NOT MET when one or more applicable assessment objectives is NOT MET.

  Satisfaction of security requirements may be accomplished by other parts of the enterprise or an External Service Provider (ESP), as defined in 32 CFR § 170.4. A security requirement is considered MET if adequate evidence is provided that the enterprise or

ESP implements the requirement objectives. An ESP may be external people, technology, or facilities that the OSA uses, including cloud service providers, managed service providers, managed security service providers, or cybersecurity-as-a-service providers.

Requirement Descriptions

Introduction

This section provides detailed information and guidance for assessing each Level 1 security requirement. The section is organized first by domain and then by individual security requirement. Each security requirement description contains the following elements as described in 32 CFR § 170.14(c):

- **Requirement Number, Name, and Statement:** Headed by the requirement identification number in the format, DD.L#-REQ (e.g., AC.L1-b.1.i); followed by the requirement short name identifier, meant to be used for quick reference only; and finally followed by the complete CMMC security requirement statement.
- **Assessment Objectives [NIST SP 800-171A]:** Identifies the specific set of objectives that must be met to receive MET for the requirement as defined in NIST SP 800-171A.
- **Potential Assessment Methods and Objects [NIST SP 800-171A]:** Describes the nature and the extent of the self-assessment actions as set forth 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 Rev. 2]:** Contains discussion from the associated NIST SP 800-171 security requirement. Level 1 aligns with FAR Clause 52.204-21, which focuses on FCI, and the NIST text has been modified, as set forth in 32 CFR § 170.15(c)(1), to reflect this.
- **Further Discussion:**
    - Expands upon the NIST SP 800-171 Rev. 2 discussion content to provide additional guidance.
    - Contains examples illustrating application of the requirements. These examples are intended to provide insight but are not intended to be prescriptive of how the requirement must be implemented, nor are they comprehensive of all assessment objectives necessary to achieve the requirement. 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.
    - Examples are written from the perspective of an organization or an employee of an organization implementing solutions or researching approaches to satisfy CMMC requirements. The objective is to put the reader into the role of implementing or maintaining alternatives to satisfy security requirements. Examples are not all-inclusive or prescriptive and do not imply any personal responsibility for complying with CMMC requirements.
    - Provides potential assessment considerations. These may include common considerations for assessing the requirement and potential questions that may be asked when assessing the objectives.

- **Key References:** Lists the identical basic safeguarding requirement from FAR clause 52.204-21 and the pertinent security requirement from NIST SP 800-171 Rev. 2.

Access Control (AC)

AC.L1-B.1.I – AUTHORIZED ACCESS CONTROL [FCI DATA]

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][3]

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][3]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan[4][5]; 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].

[3] NIST SP 800-171A, p. 9

[4] It is recommended that an OSA develop a SSP as a best practice at Level 1, however, it is not required in order to obtain a Level 1 self-assessment.

Test

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

DISCUSSION [NIST SP 800-171 REV. 2][6]

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 AC.L1-b.1.ii.

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 requirement, AC.L1-b.1.i, controls system access based on user, process, or device identity. AC.L1-b.1.i leverages IA.L1-b.1.v 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]?

[6] NIST SP 800-171 Rev. 2, p.10

- Are account requests authorized before system access is granted [d,e,f]?

KEY REFERENCES

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

AC.L1-B.1.II – TRANSACTION & FUNCTION CONTROL [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][7]

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][7]

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 REV. 2][8]

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).

[7] NIST SP 800-171A, p. 9
[8] NIST SP 800-171 Rev. 2, pp. 10-11

FURTHER DISCUSSION

Limit users to only the information systems, roles, or applications they are permitted to use and require for their roles and responsibilities. Limit access to applications and data based on 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]?
- Is access for authorized users restricted to those parts of the system they are explicitly permitted to use, that is, is access denied by default and allowed by exception (e.g., a person who only performs word-processing cannot access developer tools) [b]?

KEY REFERENCES

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

AC.L1-B.1.III – EXTERNAL CONNECTIONS [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][9]

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][9]

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 REV. 2][10]

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.

[9] NIST SP 800-171A, p. 17
[10] NIST SP 800-171 Rev. 2, pp. 15-16

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 manage connections 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

Your company has just been awarded a contract which contains FCI. You remind your coworkers of the policy requirement to use their company laptops, not personal laptops or tablets, when working remotely on this contract [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 OSAs, 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 OSA 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-B.1.IV – CONTROL PUBLIC INFORMATION [FCI DATA]

Control information posted or processed on publicly accessible information systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A][11]

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][11]

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 REV. 2][12]

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

[11] NIST SP 800-171A, p. 18
[12] NIST SP 800-171 Rev. 2, p. 16

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

Only government officials can be authorized to publicly release FCI. 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-B.1.V – IDENTIFICATION [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][13]

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][13]

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 REV. 2][14]

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

[13] NIST SP 800-171A, p. 31
[14] NIST SP 800-171 Rev. 2, p. 23

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

Individual, unique identifiers (e.g., user names) should be assigned 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 requirement, IA.L1-b.1.v, provides a vetted and trusted identity that supports the access control mechanism required by AC.L1-b.1.i.

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 contains 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 a unique user ID, which they use to log on to 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-B.1.VI – AUTHENTICATION [FCI DATA]

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][15]

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][15]

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 REV. 2][16]

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

[15] NIST SP 800-171A, p. 31
[16] NIST SP 800-171 Rev. 2, p. 23

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 a person or device is given system access, 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 a default username (e.g., admin) and password. A default username and password should be immediately changed to something unique. Default passwords may be well known to the public, easily found in a search, or easy to guess, allowing an unauthorized person to access the system.

Example 1

You are in charge of purchasing laptops that will store FCI. 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 that will transmit FCI. Upon reviewing this requirement, 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., usernames and 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 OSA 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-B.1.VII – MEDIA DISPOSAL [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][17]

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][18]

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 REV. 2][19]

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.

[17] NIST SP 800-171A, p. 41
[18] NIST SP 800-171A, p. 42
[19] NIST SP 800-171 Rev. 2, p. 29

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. NIST SP 800-88 provides guidance on media sanitization.

FURTHER DISCUSSION

Media can include 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 FCI from a 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]?

KEY REFERENCES

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

Physical Protection (PE)

PE.L1-B.1.VIII – LIMIT PHYSICAL ACCESS [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][20]

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][20]

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 REV. 2][21]

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,

[20] NIST SP 800-171A, p. 46
[21] NIST SP 800-171 Rev. 2, p. 32

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 stores FCI on computers 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 computers are 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.

Potential Assessment Considerations

- Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued [a]?
- 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]?
- Are output devices such as printers placed in areas where their use does not expose data to unauthorized individuals [c]?

KEY REFERENCES

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

PE.L1-B.1.IX – MANAGE VISITORS & PHYSICAL ACCESS [FCI DATA]

Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

ASSESSMENT OBJECTIVES [NIST SP 800-171A][22]

Determine if:

[a] visitors are escorted;

[b] visitor activity is monitored;

[c] audit logs of physical access are maintained;

[d] physical access devices are identified;

[e] physical access devices are controlled; and

[f] physical access devices are managed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A][23]

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 REV. 2][24]

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

[22] NIST SP 800-171A, p.47
[23] NIST SP 800-171A, pp. 47-48
[24] NIST SP 800-171 Rev. 2, pp. 32-33

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.

Physical access devices include keys, locks, combinations, and card readers.

FURTHER DISCUSSION

Do not allow visitors, even those people you know well, to walk around your facility without an escort. All non-employees should wear special visitor badges and/or are escorted by an employee at all times while on the property.

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.

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 1

Coming back from a meeting, you see the friend of a coworker walking down the hallway near your office where FCI is stored. 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 lunchroom [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].

Example 2

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 in which your company will receive FCI 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 [c]. 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.

Example 3

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 [f].

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]?
- Are logs of physical access to sensitive areas (both authorized access and visitor access) maintained per retention requirements [c]?
- Are visitor access records retained for as long as required [c]?
- Are lists or inventories of physical access devices maintained (e.g., keys, facility badges, key cards) [d]?
- Is access to physical access devices limited (e.g., granted to, and accessible only by, authorized individuals) [e]?
- Are physical access devices managed (e.g., revoking key card access when necessary, changing locks as needed, maintaining access control devices and systems) [f]?

KEY REFERENCES

- FAR Clause 52.204-21 b.1.ix
- NIST SP 800-171 Rev. 2 3.10.3
- NIST SP 800-171 Rev. 2 3.10.4
- NIST SP 800-171 Rev. 2 3.10.5

System and Communications Protection (SC)

SC.L1-B.1.X – BOUNDARY PROTECTION [FCI DATA]

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][25]

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][25]

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].

[25] NIST SP 800-171A, p. 53

DISCUSSION [NIST SP 800-171 REV. 2][26]

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.

It may be wise 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 with an FCI enclave. 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

[26] NIST SP 800-171 Rev. 2, p. 36

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 to 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-B.1.XI – PUBLIC-ACCESS SYSTEM SEPARATION [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][27]

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][27]

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 REV. 2][28]

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.

[27] NIST SP 800-171A, p. 55
[28] NIST SP 800-171 Rev. 2, pp. 37-38

FURTHER DISCUSSION

Publicly accessible systems should be separated from the internal systems that need to be protected. Internal systems should not be placed on the same network as publicly accessible systems, and access by default from DMZ networks to internal networks should be blocked.

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 OSAs may 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 because your network contains FCI [b]. You host the server separately from the company's internal network where FCI is stored 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-B.1.XII – FLAW REMEDIATION [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][29]

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][29]

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

[29] NIST SP 800-171A, p. 60

supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates].

DISCUSSION [NIST SP 800-171 REV. 2][30]

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. OSAs should have a process to review relevant vendor notifications and updates about problems or weaknesses. After reviewing the information, the OSA should implement a patch management process that allows for software and firmware flaws to be fixed without adversely affecting the system functionality. OSAs should define the time frames within which flaws are identified, reported, and corrected for all systems.

Example

You know that software vendors typically release patches, service packs, hot fixes, etc. and want to make sure your software that processes FCI 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].

[30] NIST SP 800-171 Rev. 2, pp. 40-41

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 within 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-B.1.XIII – MALICIOUS CODE PROTECTION [FCI DATA]

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A][31]

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][32]

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 REV. 2][33]

Designated [*appropriate*] 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,

[31] NIST SP 800-171A, p. 61
[32] NIST SP 800-171A, p. 61-62
[33] NIST SP 800-171 Rev. 2, p. 41

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 cause damage, steal information, change data, send email, show messages, or any combination of these things;
- Spyware – program designed to secretly gather information about a person's activity;
- 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 victim's data or perpetually block access to it unless a ransom is paid.

Consider use of anti-malware tools to stop or lessen the impact of malicious code.

Example

Your company's IT team is buying new computers and wants to protect your company's information from viruses and spyware. The computers will be used to process, store, and transmit FCI. They research anti-malware products, select an appropriate solution, and deploy antivirus software on all hosts for which satisfactory antivirus software is available [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-B.1.XIV – UPDATE MALICIOUS CODE PROTECTION [FCI DATA]

Update malicious code protection mechanisms when new releases are available.

ASSESSMENT OBJECTIVES [NIST SP 800-171A][34]

Determine if:

[a] malicious code protection mechanisms are updated when new releases are available.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A][35]

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 REV. 2][36]

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

[34] NIST SP 800-171A, p. 62
[35] NIST SP 800-171A, p. 62-63
[36] NIST SP 800-171 Rev. 2, pp 41-42

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 that stores FCI 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 at 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-B.1.XV – SYSTEM & FILE SCANNING [FCI DATA]

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][37]

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][37]

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 800-17]1 REV. 2[38]

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.,

[37] NIST SP 800-171A, p. 63
[38] NIST SP 800-171 Rev. 2, p. 42

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

Consider use of anti-malware software to scan for viruses in your computer systems and determine how often scans are conducted. Real-time scans look at the system whenever files are downloaded, opened, and saved. Periodic scans check previously saved files against updated malware information. Anti-malware software should be installed, run, and updated on all hosts for which satisfactory antivirus software is available.

Example

Your company transmits FCI over email. 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

Appendix A – Acronyms and Abbreviations

AC	Access Control
CD-ROM	Compact Disk Read-Only Memory
CFR	Code of Federal Regulations
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
IT	Information Technology
NIST	National Institute of Standards and Technology
OSA	Organization Seeking Assessment
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


DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
CYBERSECURITY MATURITY MODEL
CERTIFICATION