CMMC REPORTS MASTER LIST BASED ON CMMC & SP 800-171A

This is a mashup of CMMC requirements, references to SP 800-171 (using language found in Rev 2), and testing requirements found in SP 800-171A. The output aligns control language with applicable testing requirements.

VERSION 2020.05.24
CREATED BY
CHRISTOPHER DAVIS

AC: Access Control C001:AC.1.001

Maturity Level 1

Capability C001: Establish system access requirements

Practice AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Discussion: [DRAFT NIST SP 800-171 R2]: Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2 (AC.1.002).

CMMC Clarification: Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

Example 1

You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

Example 2

A coworker from the marketing department tells you their boss wants to buy a new multifunction 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 stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

Mapping

- NIST SP 800-53R4: AC-2, AC-3, AC-17
- NIST SP 800-171: 3.1.1
- CIS: 1.4,1.6,5.1,14.6,15.10,16.8,16.9,16.11
- CSF: PR.AC-1,PR.AC-3,PR.AC-4,PR.AC-6,PR.PT-3,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

NIST SP 800-171R2 Related Discussion: 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 non-privileged) are addressed in requirement 3.1.2.

Assessment

Assessment Objective(s): Determine if:

3.1.1[a] authorized users are identified.

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

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

3.1.1[d] system access is limited to authorized users.

3.1.1[e] system access is limited to processes acting on behalf of authorized users.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 1

Capability C002: Control internal system access

Practice AC.1.002: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-ofweek, 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).

CMMC Clarification: Make sure to limit users/employees to only the information systems, roles, or applications they are permitted to use and that are needed for their jobs.

Example

You are in charge of payroll for the company and need access to certain company financial information and systems. You work with IT to set up the system so that when users log onto the company's network, only those employees you allow can use the payroll applications and access payroll data. Because of this good access control, your coworkers in the Shipping Department cannot access information about payroll or paychecks.

Mapping

- NIST SP 800-53R4: AC-2, AC-3, AC-17
- NIST SP 800-171: 3.1.2
- CIS: 1.4,1.6,5.1,8.5,14.6,15.10,16.8,16.9,16.11
- CSF: PR.AC-1,PR.AC-3,PR.AC-4,PR.AC-6,PR.PT-3,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Limit system access to the types of transactions and functions that authorized users are permitted to execute.

NIST SP 800-171R2 Related Discussion: 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-oforigin. 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).

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing access control policy].

Testing Assessment Notes:

Maturity Level 1

Capability C004: Limited access to authorized users and processes

Practice AC.1.003: Verify and control/limit connections to and use of external information systems.

Discussion: [DRAFT NIST SP 800-171 R2]: External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privatelyowned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of Federally Contracted Information, 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 Federally Contracted Information across an organization, the organization may have systems that process Federally Contracted Information and others that do not. And among the systems that process Federally Contracted Information there are likely access restrictions for Federally Contracted Information that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.

CMMC Clarification: Make sure to control and manage connections between your company network and outside networks, such as the public internet or a network that does not belong to your company. Be aware of applications that can be run by outside systems. Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information. You can also choose to limit how and when your network is connected to outside systems and/or decide that only certain employees can connect to outside systems from network resources.

Example

You help manage IT for your employer. You and your coworkers are working on a big proposal, and all of you will put in extra hours over the weekend to get it done. Part of the proposal includes Federal

Contract Information, or FCI. FCI is information that you or your company get from doing work for the Federal government. Because FCI is not shared publicly, you remind your coworkers to use their company laptops, not personal laptops or tablets, when working on the proposal over the weekend.

Mapping

- NIST SP 800-53R4: AC-20, AC-20(1)
- NIST SP 800-171: 3.1.20
- CIS: 12.1,12.4
- CSF: ID.AM-4,PR.AC-3

NIST SP 800-171R2 Related Security Requirement: Verify and control/limit connections to and use of external systems.

NIST SP 800-171R2 Related Discussion: External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, 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 CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.

Assessment

Assessment Objective(s): Determine if:

3.1.20[a] connections to external systems are identified.

3.1.20[b] the use of external systems is identified.

3.1.20[c] connections to external systems are verified.

3.1.20[d] the use of external systems is verified.

3.1.20[e] connections to external systems are controlled/limited.

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

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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].

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 1

Capability C004: Limited access to authorized users and processes

Practice AC.1.004: Control information posted or processed on publicly accessible information systems.

Discussion: [DRAFT NIST SP 800-171 R2]: In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI 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.

CMMC Clarification: Do not allow sensitive information, including Federal Contract Information (FCI), which may include CUI, to become public. It is important to know which users/employees are allowed to publish information on publicly accessible systems, like your company website. Limit and control information that is posted on your company's website(s) that can be accessed by the public.

Example

You are head of marketing for your company and want to become better known by your customers. So, you decide to start issuing press releases about your company projects. Your company gets FCI from doing work for the Federal government. FCI is information that is not shared publicly. Because you recognize the need to control sensitive information, including FCI, you carefully review all information before posting it on the company website or releasing to the public. You allow only certain employees to post to the website.

Mapping

- NIST SP 800-53R4: AC-22
- NIST SP 800-171: 3.1.22
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Control CUI posted or processed on publicly accessible systems.

NIST SP 800-171R2 Related Discussion: 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, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI 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.

Assessment

Assessment Objective(s): Determine if:

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

3.1.22[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.

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

3.1.22[d] content on publicly accessible systems is reviewed to ensure that it does not include CUI.

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

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C001: Establish system access requirements

Practice AC.2.005: Provide privacy and security notices consistent with applicable CUI rules.

Discussion: [DRAFT NIST SP 800-171 R2]: System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

CMMC Clarification: Every system has legal information about user privacy and security. A system-use notification banner displays the legal requirements of using the systems. Users are required to click to agree to the displayed requirements of using the system each time they logon to the machine. You can use this implicit agreement in the civil and/or criminal prosecution of an attacker that violates the terms.

Discuss legal notification requirements with your organization's legal counsel. This will ensure that they meet all applicable requirements. You should inform the user that:

- you may monitor, record, and subject to audit any information system usage;
- you prohibit unauthorized use of the information system;
- you may subject unauthorized use to criminal and civil penalties; and
- use of the information system indicates consent to monitoring and recording.

Example

You are setting up IT equipment for your organization. You have worked with legal counsel to draft a notification. The system displays the required security and privacy information when anyone logs on to your organization's machines. You ensure that this notification displays to all users of all of the organization's machines.

Mapping

- NIST SP 800-53R4: AC-8
- NIST SP 800-171: 3.1.9
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Provide privacy and security notices consistent with applicable CUI rules.

NIST SP 800-171R2 Related Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications

are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

Assessment

Assessment Objective(s): Determine if:

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

3.1.9[b] privacy and security notices are displayed.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing system use notification].

Testing Assessment Notes:

Maturity Level 2

Capability C001: Establish system access requirements

Practice AC.2.006: Limit use of portable storage devices on external systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while "external" typically refers to outside of the organization's direct supervision and authority that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

CMMC Clarification: A portable storage device is a system component that you can insert and remove from a system. You use it to store data or information. Examples of portable storage devices include:

- floppy disks;
- compact/digital video disks (CDs/DVDs);
- flash/thumb drives;
- external hard disk drives; and
- flash memory cards/drives that contain nonvolatile memory.

You can put this practice in place two ways:

- set up a policy that describes the usage restrictions of these devices or
- establish technical means, such as configuring devices to work only when connected to a system to which they can authenticate.

Example

Your organization has a usage restriction policy. It states that users cannot use portable storage devices in external information systems without management approval.

Mapping

- NIST SP 800-53R4: AC-20(2)
- NIST SP 800-171: 3.1.21
- CIS: 13.7,13.8,13.9
- CSF: ID.AM-4,PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Limit use of portable storage devices on external systems.

NIST SP 800-171R2 Related Discussion: Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C002: Control internal system access

Practice AC.2.007: Employ the principle of least privilege, including for specific security functions and privileged accounts.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

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

CMMC Clarification: You should apply the principle of least privilege to all users and processes on all systems. This means you assign the fewest permissions necessary for the user or process to accomplish their business function. Also, you:

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

Example

As the IT administrator for your organization, you create accounts. You apply the fewest privileges necessary for the user or process to complete their task. This means you assign everyone a basic user role. This prevents a user from modifying system configurations. You also assign privileged access only to users and processes that need it, such as IT staff.

Mapping

- NIST SP 800-53R4: AC-6, AC-6(1), AC-6(5)
- NIST SP 800-171: 3.1.5
- CIS: 14.6
- CSF: PR.AC-4

NIST SP 800-171R2 Related Security Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

NIST SP 800-171R2 Related Discussion: Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

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

Assessment

Assessment Objective(s): Determine if:

3.1.5[a] privileged accounts are identified.

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

3.1.5[c] security functions are identified.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C002: Control internal system access

Practice AC.2.008: Use non-privileged accounts or roles when accessing nonsecurity functions.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and nonprivileged account.

CMMC Clarification: A user with a privileged account can perform more tasks and access more information than a person with a non-privileged account. This means that tasks performed when using the privileged account can have a greater impact on the system. You restrict administrator use of privileged accounts. Only those who perform a function that requires more access have a privileged account. This reduces the risk of unintentional harm to systems and data.

Example

As the IT administrator for your organization, you have two user accounts. One is a nonprivileged account, which you use when performing non-privileged duties. These tasks include sending or receiving emails. The other is a privileged account, which you use only when performing administrative functions. Examples include troubleshooting a device or setting up new user accounts.

Mapping

- NIST SP 800-53R4: AC-6(2)
- NIST SP 800-171: 3.1.6
- CIS: 4.3,4.6
- CSF: PR.AC-4

NIST SP 800-171R2 Related Security Requirement: Use non-privileged accounts or roles when accessing nonsecurity functions.

NIST SP 800-171R2 Related Discussion: This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Assessment

Assessment Objective(s): Determine if:

3.1.6[a] nonsecurity functions are identified.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing least privilege functions].

Testing Assessment Notes:

Maturity Level 2

Capability C002: Control internal system access

Practice AC.2.009: Limit unsuccessful logon attempts.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

CMMC Clarification: Consecutive, unsuccessful logon attempts may indicate malicious activity. You can mitigate these types of attacks by limiting the number of unsuccessful logon attempts. There are many ways to do this. Having three consecutive, unsuccessful logon attempts is a common setting. Organizations should set this number at a level that fits their risk profile. Fewer unsuccessful attempts provide higher security.

After the system locks an account, it has several options to unlock it. The most common is to keep the account locked for a predefined time. After that time, the account unlocks. Another option is to keep the account locked until an administrator unlocks it.

Example

You attempt to log on to your work computer. You mistype your password three times in a row. You call your IT help desk or administrator. The administrator tells you your account is locked. He explains that all passwords lock after three unsuccessful logon attempts. This limits the effectiveness of brute-force and other password attacks. He tells you he can unlock it, or you can wait five minutes and the account will unlock automatically.

Mapping

- NIST SP 800-53R4: AC-7
- NIST SP 800-171: 3.1.8
- CIS:
- CSF: PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Limit unsuccessful logon attempts.

NIST SP 800-171R2 Related Discussion: This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

Assessment

Assessment Objective(s): Determine if:

3.1.8[a] the means of limiting unsuccessful logon attempts is defined.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C002: Control internal system access

Practice AC.2.010: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Discussion: [DRAFT NIST SP 800-171 R2]: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

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

CMMC Clarification: You can set session locks on your system. A user can enable the lock. Also, the system can enable it automatically after a preset time, for example, from one to five minutes. Session locks are a quick way to prevent unauthorized use of the systems without having a user log off.

A locked session shows pattern-hiding information on the machine screen. This masks the data on the display.

Example

You are the IT administrator in your organization. You notice that employees leave their offices without locking their computers. Sometimes their screens display sensitive company information. You remind your coworkers to lock their systems when they walk away. You set all machines to lock after five minutes of inactivity.

Mapping

- NIST SP 800-53R4: AC-11, AC-11(1)
- NIST SP 800-171: 3.1.10
- CIS: 16.11
- CSF:

NIST SP 800-171R2 Related Security Requirement: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

NIST SP 800-171R2 Related Discussion: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

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

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C002: Control internal system access

Practice AC.2.011: Authorize wireless access prior to allowing such connections.

Discussion: [DRAFT NIST SP 800-171 R2]: Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

CMMC Clarification: You should base the use of wireless technologies on approved guidelines from management. These guidelines may include the following:

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

Example

Your company is implementing a wireless network at their headquarters. You work with management to draft policies about the use of the wireless network. You allow only company-approved devices that contain verified security configuration settings. Also, you write usage restrictions to follow for anyone who wants to use the wireless network.

Mapping

- NIST SP 800-53R4: AC-18
- NIST SP 800-171: 3.1.16
- CIS: 15.1,15.10
- CSF: PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Authorize wireless access prior to allowing such connections.

NIST SP 800-171R2 Related Discussion: Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

Assessment

Assessment Objective(s): Determine if:

3.1.16[a] wireless access points are identified.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C003: Control remote system access

Practice AC.2.013: Monitor and control remote access sessions.

Discussion: [DRAFT NIST SP 800-171 R2]: Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

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

CMMC Clarification: Remote access connections pass through untrusted networks and should therefore not be trusted without proper security controls in place. All remote access should implement approved encryption. This ensures the confidentiality of the data. Check connections to ensure that only authorized users and devices are connecting. Monitoring may include tracking who is accessing the network remotely and what files they are accessing during the remote session.

Example

You work from remote locations, such as your house or a client site and need access to your company's network. The IT administrator issues you a company laptop with a VPN software installed which is required to connect to the network remotely. After you connect to the VPN, you must accept a privacy notice which states that the company's security department may monitor your connection. They do this through the use of a network-based Intrusion Detection System (IDS). They also review audit logs to see who is connecting remotely and when. Next you see the message "Verifying compliance." This means the system is checking your device to ensure it meets the established requirements to connect. The administrator explains that after your machine connects to the network using the VPN, you can have confidence that your session is private because your company implements approved encryption.

Mapping

- NIST SP 800-53R4: AC-17(1)
- NIST SP 800-171: 3.1.12
- CIS: 12.11,12.12

- CSF: PR.AC-3,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Monitor and control remote access sessions.

NIST SP 800-171R2 Related Discussion: Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyberattacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

Assessment

Assessment Objective(s): Determine if:

3.1.12[a] remote access sessions are permitted.

3.1.12[b] the types of permitted remote access are identified.

3.1.12[c] remote access sessions are controlled.

3.1.12[d] remote access sessions are monitored.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C003: Control remote system access

Practice AC.2.015: Route remote access via managed access control points.

Discussion: [DRAFT NIST SP 800-171 R2]: Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

CMMC Clarification: You can limit the number of remote access control points. This reduces the attack surface for organizations. Route all remote access sessions through as few points as possible. This:

- allows for better visibility into the traffic coming into the network;
- simplifies network management; and
- increases the ability to monitor and control the connections.

Example

You are the IT administrator for a company with many locations. Several employees at different locations need to connect to the network while working remotely. Each location has its own connection to the internet. Since each company location has a direct connection to headquarters, you decide to route all remote access through the headquarters location. All remote traffic comes to one location. You have to monitor the traffic on only one device, rather than one per location. The company will not have to buy as much equipment.

Mapping

- NIST SP 800-53R4: AC-17(3)
- NIST SP 800-171: 3.1.14
- CIS: 15.5,15.10
- CSF: PR.AC-3,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Route remote access via managed access control points.

NIST SP 800-171R2 Related Discussion: Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

Assessment

Assessment Objective(s): Determine if:

3.1.14[a] managed access control points are identified and implemented.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C004: Limited access to authorized users and processes

Practice AC.2.016: Control the flow of CUI in accordance with approved authorizations.

Discussion: [DRAFT NIST SP 800-171 R2]: Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

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

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

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

In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes: prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

CMMC Clarification: Flow control regulates where and how information can flow. Firewalls and proxy servers can be used to control traffic flow. Typically, organizations will have a firewall between the internal network and the internet. Often multiple firewalls are used inside a network to create zones to separate sensitive data, business units or user groups. Proxy servers can be used to break the connection between multiple networks. All traffic entering or leaving a network is intercepted by the proxy, preventing direct access between networks. This can have security and performance benefits.

Additionally, organizations should ensure that all sensitive information is encrypted before being transmitted over the internet.

Example

You configure a proxy device on your company's network. Your goal is to better mask and protect the devices inside your network. After you configure the device, information does not flow directly from the internal network to the internet. The proxy system intercepts the traffic. Then, the proxy analyzes it to determine if it is legitimate. If it is, the system allows it on the network and sends it to its destination.

Mapping

- NIST SP 800-53R4: AC-4
- NIST SP 800-171: 3.1.3
- CIS: 12.1,12.2,12.5,12.8,13.3,14.1,14.6,14.7
- CSF: ID.AM-3,PR.AC-5,PR.DS-5,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Control the flow of CUI in accordance with approved authorizations.

NIST SP 800-171R2 Related Discussion: Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping exportcontrolled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

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

Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes: prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Assessment

Assessment Objective(s): Determine if:

3.1.3[a] information flow control policies are defined.

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

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

3.1.3[d] authorizations for controlling the flow of CUI are defined.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C002: Control internal system access

Practice AC.3.017: Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Discussion: [DRAFT NIST SP 800-171 R2]: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

CMMC Clarification: A company must avoid situations in which conflicts of interest or even lack of knowledge can create security problems. This can be accomplished by splitting important duties and tasks between employees in order to reduce intentional or unintentional execution of malicious activities, when those involved are not colluding. This allows the organization to minimize employees' fraud, abuse and errors. Summarizing, no one person should be in charge of an entire critical task from beginning to end.

Example

You are responsible for designing and implementing security solutions in your organization. The same person should not test security mechanisms, conduct security audits, and release software for delivery. Policy is created and implemented so that the development team does not do testing and the test team does not do development. This eliminates your ability to intentionally or unintentionally develop a weak security solution that is not identified through testing or is released prematurely before unit, integration, regression, operational and security testing are complete.

Mapping

- NIST SP 800-53R4: AC-5
- NIST SP 800-171: 3.1.4
- CIS:
- CSF: PR.AC-4

NIST SP 800-171R2 Related Security Requirement: Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

NIST SP 800-171R2 Related Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management,

quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

Assessment

Assessment Objective(s): Determine if:

3.1.4[a] the duties of individuals requiring separation are defined.

3.1.4[b] responsibilities for duties that require separation are assigned to separate individuals.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C002: Control internal system access

Practice AC.3.018: Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Discussion: [DRAFT NIST SP 800-171 R2]: Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2 (AC.1.002).

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

CMMC Clarification: Non-privileged users should not be given permissions other than those required to do their basic job functions. Privileged users are granted additional permissions. They are employees given authorization to perform certain privileged functions involving the control, monitoring, or administration of the system including security functions. When these special privileged functions are performed, the activity should be captured in an audit log which can be used to identify abuse. Non-privileged employees should not be granted permission to perform any of the functions of a privileged user.

Example

As a system administrator for your organization you have security controls in place that prevent non-privileged users from performing privileged activities. However, you accidentally gave a standard user elevated system administrator privileges. The organization has implemented an endpoint detection and response solution that provides visibility into the use of privileged activities. This monitoring system logs the use of administrative privileges by an unapproved user allowing you to correct the error.

Mapping

- NIST SP 800-53R4: AC-6(9), AC-6(10)
- NIST SP 800-171: 3.1.7
- CIS:
- CSF: PR.AC-4

NIST SP 800-171R2 Related Security Requirement: Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

NIST SP 800-171R2 Related Discussion: Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Nonprivileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2.

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

Assessment

Assessment Objective(s): Determine if:

3.1.7[a] privileged functions are defined.

3.1.7[b] non-privileged users are defined.

3.1.7[c] non-privileged users are prevented from executing privileged functions.

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

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Access control policy; procedures addressing least privilege; system security plan; system design documentation; list of privileged functions and associated user account assignments; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C002: Control internal system access

Practice AC.3.019: Terminate (automatically) user sessions after a defined condition.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

CMMC Clarification: This practice may require security policy development if it does not exist. Configure the system to end user sessions based on the organization's policy. Policy guidance for session termination usually includes circumstances, events, or specific triggers that require automatically terminating the session or logging off the user. If there is no automatic control of user sessions, an attacker can take advantage of an unattended session.

Example 1

You are the system administrator for your organization and were given the task to implement the termination of all user sessions after 1 hour of inactivity. As the session timeout approaches, the system prompts users with a warning banner asking if they want to continue the session. When the session timeout does occur, the login page pops-up and the users must login to start a new session.

Example 2

You are logged into a corporate database containing CUI, but you are not authorized to view CUI. You have submitted a series of complex queries that violate policy, as they appear to be an attempt to extract CUI you are not authorized to view. Your session is terminated as a result of what appears to be a large query set attack, a violation of corporate policy. You must reestablish the session before you can submit additional legitimate queries.

Mapping

- NIST SP 800-53R4: AC-12
- NIST SP 800-171: 3.1.11
- CIS: 16.7,16.11
- CSF:

NIST SP 800-171R2 Related Security Requirement: Terminate (automatically) a user session after a defined condition.

NIST SP 800-171R2 Related Discussion: This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

Assessment

Assessment Objective(s): Determine if:

3.1.11[a] conditions requiring a user session to terminate are defined.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing user session termination].

Testing Assessment Notes:

Maturity Level 3

Capability C002: Control internal system access

Practice AC.3.012: Protect wireless access using authentication and encryption.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems.

CMMC Clarification: Use a combination of authentication and encryption methods to protect the access to wireless networks. Authenticating users to a Wireless Access Point can be done in numerous ways. One approach uses shared key authentication based on a Pre-Shared Key. Another possibility uses Network Extensible Authentication Protocol (EAP) based on an authentication server (such as a Remote Authentication Dial-In User Service (RADIUS) server) and a mechanism to enforce port-based network access control. Open authentication should not be used because it authenticates any user, and at best, logs the MAC address, which is easily spoofed.

Example

You are responsible for protecting the data in your organization by configuring the Wireless Access Point to enforce authentication. Before users gain access to your network, they must authenticate by demonstrating possession of a pre-shared key (typically used in smaller companies) before crypto keys can be installed; or by passing credentials to a RADIUS server (typically used in larger organizations) before the access port is opened.

Mapping

- NIST SP 800-53R4: AC-18(1)
- NIST SP 800-171: 3.1.17
- CIS: 15.7,15.8
- CSF: PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Protect wireless access using authentication and encryption.

NIST SP 800-171R2 Related Discussion: Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See [NIST CRYPTO].

Assessment

Assessment Objective(s): Determine if:

3.1.17[a] wireless access to the system is protected using authentication.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C002: Control internal system access

Practice AC.3.020: Control connection of mobile devices.

Discussion: [DRAFT NIST SP 800-171 R2]: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements.

CMMC Clarification: Organizations should establish guidelines and acceptable practices for the proper configuration and use of mobile devices. First the device must be identified. The availability of a unique identifier is going to depend on the device vendor, and the openness of the vendor's API, whether or not the device is under EMM/MDM control and, if so, the approach used by the developer of the EMM/MDM. There are many different types of identifiers (e.g., UDID, UUID, Android ID, IMEI, MAC Address, serial number, MDM generated ID) that can be used to identify the device, and an organization must choose an approach that applies under their specific circumstances. Once the device is identified and authenticated, it is checked to ensure it complies with appropriate configuration settings and software versions for the operating system and applications. At the same time the device is checked to ensure anti-virus software is running with current definitions. Finally, hardware configurations are checked to ensure any disallowed features are turned off.

Example

Your organization has a policy that provides guidelines for using mobile devices such as iPads, tablets, mobile phones, PDAs. It states that all mobile devices must be approved and registered with the IT department before connecting to the network. The IT department uses a Mobile Device Management solution to monitor mobile devices and enforce policies across the enterprise.

Mapping

- NIST SP 800-53R4: AC-19
- NIST SP 800-171: 3.1.18

- CIS: 13.6,16.7
- CSF: PR.AC-3,PR.AC-6

NIST SP 800-171R2 Related Security Requirement: Control connection of mobile devices.

NIST SP 800-171R2 Related Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements.

Assessment

Assessment Objective(s): Determine if:

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

3.1.18[b] mobile device connections are authorized.

3.1.18[c] mobile device connections are monitored and logged.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C003: Control remote system access

Practice AC.3.014: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Discussion: [DRAFT NIST SP 800-171 R2]: Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography.

CMMC Clarification: A remote access session involves logging in to the organization's network from a remote location such as home or an alternate work site. This remote access session must be secured using FIPS-validated cryptography to provide confidentiality and prevent anyone from capturing session information exchanges.

Example

As the IT administrator for your organization you are responsible for implementing a remote network access capability for users that work offsite. In order to provide session confidentiality, you decide to establish a TLS based Virtual Private Network mechanism. You chose a product that has completed FIPS validation. You require user authentication rather than mutual authentication, but you also set up two factor authentication based on a token passcode and a user PIN before the VPN is established.

Mapping

- NIST SP 800-53R4: AC-17(2)
- NIST SP 800-171: 3.1.13
- CIS: 15.7,15.8
- CSF: PR.AC-3,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

NIST SP 800-171R2 Related Discussion: Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; [NIST CMVP]; National Security Agency Cryptographic Standards.

Assessment

Assessment Objective(s): Determine if:

3.1.13[a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C003: Control remote system access

Practice AC.3.021: Authorize remote execution of privileged commands and remote access to security-relevant information.

Discussion: [DRAFT NIST SP 800-171 R2]: A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

CMMC Clarification: Privileged users need to execute commands with elevated privileges. But not all privileged users are allowed to perform these functions from a remote location, and not all privileged commands can be executed remotely. You must document which user roles have permissions to remotely execute privileged commands to make changes and to access security relevant information. In addition, you must document which administrative functions can be executed remotely. This documentation must be used to establish security mechanisms that enforce the policy.

Example

In accordance with the Access Control Policy certain users may be permitted to perform a limited set of administrative commands from a remote machine. Implement controls to enforce 1) who can remotely execute a privileged command and which privileged commands they can execute, and 2) who is allowed access to security relevant information such as audit log configuration settings.

Mapping

- NIST SP 800-53R4: AC-17(4)
- NIST SP 800-171: 3.1.15
- CIS: 8.8,12.11,12.12
- CSF: PR.AC-3,PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Authorize remote execution of privileged commands and remote access to security-relevant information.

NIST SP 800-171R2 Related Discussion: A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant

information. Securityrelevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

Assessment

Assessment Objective(s): Determine if:

3.1.15[a] privileged commands authorized for remote execution are identified.

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

3.1.15[c] the execution of the identified privileged commands via remote access is authorized.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing remote access management].

Testing Assessment Notes:

Maturity Level 3

Capability C004: Limited access to authorized users and processes

Practice AC.3.022: Encrypt CUI on mobile devices and mobile computing platforms.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including encrypting selected data structures such as files, records, or fields. Protecting cryptographic keys is an essential element of any encryption solution.

CMMC Clarification: Ensure CUI is encrypted using approved and validated algorithms for full disk encryption (FDE) or container-based encryption on all mobile devices and platforms to include smartphones, tablets, E-readers, and notebook computers. Mobile phones will typically encrypt a virtual container on the device; CUI should be held within the secure encrypted container. A laptop will typically use FDE. One big advantage of using encrypted containers on smartphones is applications and temporary files are not encrypted, preserving battery life that would otherwise be shortened by unnecessary cryptographic operations.

Example

You are in charge of implementing encryption for your organization. One of the encryption methods you chose for mobile devices is full disk encryption to encrypt all files, folders and volumes. When an individual checks out digital media and leaves the building a thief who obtains the media cannot access the information since everything on the disk is encrypted. Similarly, all CUI on a smartphone is put in a secure encrypted container, and if a phone containing CUI is lost, an adversary cannot recover it.

Mapping

- NIST SP 800-53R4: AC-19(5)
- NIST SP 800-171: 3.1.19
- CIS: 13.6
- CSF: PR.AC-3

NIST SP 800-171R2 Related Security Requirement: Encrypt CUI on mobile devices and mobile computing platforms.

NIST SP 800-171R2 Related Discussion: Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including encrypting selected data structures such as files, records, or fields. See [NIST CRYPTO].

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 4

Capability C002: Control internal system access

Practice AC.4.023: Control information flows between security domains on connected systems.

Discussion: [DRAFT NIST SP 800-171B (MODIFIED)]: Organizations employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services; provide a packet-filtering capability based on header information; or provide message-filtering capability based on message content.

Transferring information between systems in different security domains with different security policies introduces risk that the transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between connected systems. Organizations mandate specific architectural solutions when required to enforce logical or physical separation between systems in different security domains. Enforcement includes prohibiting information transfers between connected systems; employing hardware mechanisms to enforce one-way information flows; and verifying write permissions before accepting information from another security domain or connected system.

CMMC Clarification: This practice is not concerned with classified security domains. It addresses information flow among domains containing CUI and those that do not. While access control is concerned with controlling access to information by users and processes, controlling information flow (information flow control) is concerned with where information is allowed to move within a system and between systems. In general, information flow control can apply to any needed flow restrictions. For this CMMC practice the flows of concern are primarily between CUI authorized and CUI not-authorized components/systems. Any attempt to move CUI to a domain that has not been designated as a domain allowed to store or process CUI must be blocked.

Example 1

You are the IT administrator for your organization. You have designed the network in each of the regional offices to have two zones: one zone that can store and process CUI data and a second zone where CUI information is not permitted. A firewall separates the two zones in the office so staff cannot access files and resources within the office, and a site-to-site VPN over the corporate WAN allows the CUI zones to communicate. To ensure separation between CUI projects, staff are given file access permissions to project servers and file stores by project. To facilitate the transfer of CUI files and data between the same project team working in each regional office, you install a SharePoint server on the CUI zone of the headquarters office. Authorized staff have accounts and use their MFA token to log into the SharePoint server to view or modify projects files stored there.

Mapping

- NIST SP 800-53R4: AC-4, AC-4(1), AC-4(6), AC-4(8), AC-4(12), AC-4(13), AC-4(15), AC-4(20), SC-46
- NIST SP 800-171:
- CIS: 12.1,12.2,13.1,13.3,14.1,14.2,14.5,14.6,14.7,15.6,15.1
- CSF: ID.AM-3,PR.AC-5,PR.DS-5,PR.PT-4,DE.AE-1

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C002: Control internal system access

Practice AC.4.025: Periodically review and update CUI program access permissions.

Discussion: [CMMC]: Organizations must maintain the authorizations for access to CUI information on a regular basis, considering whether existing authorizations are still needed or new authorization are required, and update the authorizations accordingly. Reviews of access take into consideration mission/business needs and maintain the organization's implementation of the principle of least privilege.

CMMC Clarification: Users must have organizational approval to read, write and process CUI associated with a program, and the organization must maintain an authoritative list of who has been granted access to CUI. Review and update ACLs and/or appropriate access methods periodically (as determined by the organization, but at least annually) to maintain accurate permission sets when employees' roles change.

Example

You manage IT for your organization. When a new employee joined the organization, they were granted complete access to CUI for the project they were working on. A few months later, their role changed when they are moved to a different project owned by the same program manager but no longer requiring access to CUI. During the periodic review of the access control configuration, you compare the results to the official permission baseline held by the program manager. You determine that the employee should no longer have access to CUI. You revoke the CUI access permissions of the user.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C003: Control remote system access

Practice AC.4.032: Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role.

Discussion: [CMMC]: This practice adds additional granularity to remote access restrictions based upon organization-determined factors. The example factors in the practice are provided to help explain the meaning of 'risk factors' as anything that adds additional context to be considered in a determination of whether to grant remote access.

The intent of this practice is to define additional context for allowed remote access and then to enforce via technical, versus just policy, means.

CMMC Clarification: This practice adds context about the user and the specific access attempt before network access is granted. First, the organization must identify attributes that are important for managing the risk of remote network access. Then, the administrator restricts remote access based on the state of these attributes. The remote access control mechanism must be enhanced to check the attributes such as the subject's location, the state of the network (e.g., running services, resources available, traffic statistics, network hosts in the local network and traffic patterns between nodes), host posture, time-of-day, expected behavior associated with the user's role, and normal behavior for the user based on previous use. All the attributes checked must be within tolerance for the user requesting remote access. The organization is not limited to these attributes or required to use these attributes.

One possible approach could include:

a policy database or the organization determined access policy;

an attribute database for subjects, the environment and resources; and

a policy enforcement engine leveraging a policy language like XACML to check the policy and attributes before access is granted.

Example

You are an employee who typically works from home using a corporately owned laptop. You request access from your laptop to a server containing network diagrams for a system you are designing, and access is granted. You also have a personal tablet which you only use for email via a corporate web site when travelling to a sponsor's location. Since you are traveling more and more frequently, you request access to the server using the tablet to support your engineering work. Since the device is personally owned, the host posture attribute is not satisfied. As a result your network access request from the tablet is denied.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:

- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C002: Control internal system access

Practice AC.5.024: Identify and mitigate risk associated with unidentified wireless access points connected to the network.

Discussion: [CMMC]: Unidentified and unauthorized wireless access points can be connected to a network by authorized users trying to extend the network or by malicious users. They may allow unauthorized users direct access to an organization's network. In either case they represent a cybersecurity vulnerability. Organizations must mitigate this vulnerability.

CMMC Clarification: This practice can be implemented in a variety of ways. One approach would be to use a Wireless Intrusion Detection System (WIDS), a network device that monitors the radio spectrum for the presence of unauthorized access points. Other approaches are those used to detect and/or block any rogue network device. On the physical security side, unused RJ45 jacks in a facility can be turned off, however, this does not account for repurposing an authorized jack. A more robust solution is to identify authorized devices and create access controls limiting connections to those devices. Each device that is allowed to connect has a profile to include expected physical location that is maintained by the system administrators. This, in turn, facilitates the creation of a device white list which can be used with a port monitoring tool to control connections. Another approach would be the utilization of device detection software that the system administrator uses to establish a device baseline which is periodically compared to new scans using the same software to identify changes, specifically unauthorized additions when compared to the scan result of authorized connected devices.

Example 1

You are a security engineer and the organization has implemented a WIDS. The WIDS detects signals from an unauthorized access point and sends an alert. You investigate and verify the unauthorized access point exists on the network. You work with the network team to block all traffic on the network (both into and out of the access point) until the device can be located and removed.

Example 2

You are a network engineer at your organization. You have noticed that there is a new device on the network that has not been profiled. You use the information from your network diagrams and your tools to identify the office where the port terminates. Using this information, you look in your database and learn that it is normally a printer that plugs into that port. Your network tools do not show the printer on the network. You disable the network port and visit the office. When you arrive, you find that a network printer has been unplugged and an unapproved access point has been plugged into it's port. The employee in the office says that they needed better wireless access in the office so they brought in the access point from home and plugged it in. You explain that this is against company policy, unplug their access point, and plug the printer back into the port. Returning to your desk, you follow the security incident process for reporting the policy violation before reactivating the network port.

Mapping

- NIST SP 800-53R4: SI-4(14)

- NIST SP 800-171:
- CIS: 15.3
- CSF: PR.DS-5,DE.AE-1,DE.CM-7

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C005: Identify and document assets

Practice AM.3.036: Define procedures for the handling of CUI data.

Discussion: [CMMC]: The organization should define procedures for the proper handling of CUI. These procedures typically involve establishing controls to protect and sustain sensitive information. Examples of controls an organization may implement through data handling procedures include policies (data categorization, protection, disposal, backup), access controls for data, regular backups and physical security protections.

CMMC Clarification: Establish procedures for handling CUI. Procedures should include how to categorize data as CUI and how to provide and enforce access control for CUI. It also includes guidance on how to receive, transmit, store, and destroy CUI. The procedures should account for both physical and digital CUI.

Example

As a manager for a government program that contains CUI, you have established procedures for handling government identified CUI. These procedures account for both physical and digital CUI, and include:

- identification of CUI when provided government labeling and guidance;
- controlled environments to protect CUI (e.g., put it in a designated system or folder);
- steps to reasonably ensure that unauthorized individuals cannot access CUI; and
- protections for the confidentiality of CUI (e.g., electronic or physical CUI when in transit).

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C006: Manage asset inventory

Practice AM.4.226: Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.

Discussion: [CMMC]: Organizations employ systems that can assess assets connected to the network in real time, or can create an inventory identifying system-specific information required for component accountability and to provide support to identify, control, monitor, and verify configuration items in accordance with the authoritative source. For user computing systems this should include: firmware level, OS type, drive type, network and wireless card vendors, monitor card type and vendor, and software applications installed on that system.

CMMC Clarification: One purpose an organization might have in determining the component attributes is to identify and locate specific systems in the event a vulnerability is discovered in the hardware or software installed so patches can be rapidly deployed to these systems or have the systems isolated from the network. For small organizations or small enclaves, this might be achieved with manual processes. Automation is expected as scale increases in order to achieve results in an operational meaningful timeframe.

Example 1

You are an IT administrator for your organization. You learn from the vendor about a privilege escalation vulnerability in version 9.3.201 of an application when running on macOS 10.14. Since you have this version of the application installed at your organization, you download the patch the vendor has released to correct this vulnerability. You run a report to identify all the macOS 10.14 systems with this version the software application installed. You schedule a job to install the patch the next time each of the systems on the report connects to the network.

Example 2

You are on the cyber hunt team and find out there is a technique in the wild that adversaries are using against an IoT sensor that your organization has deployed. You check your system to identify how many of these sensors are currently connected to the network and their IP Addresses. You provide this information to the cyber operations team for increased monitoring until the vendor releases a patch.

Mapping

- NIST SP 800-53R4: CM-8
- NIST SP 800-171:
- CIS: 1.1,1.2,1.4,1.5,2.3,2.4,2.5
- CSF: ID.AM-1,ID.AM-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C007: Define audit requirements

Practice AU.2.041: Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of VoIP.

CMMC Clarification: You need to capture information in audit logs. This ensures that you can trace the actions you audit to a specific user. This may include capturing information from users, including:

- user IDs;
- source and destination addresses; and
- time stamps.

Such information helps track actions to an individual.

Example

You are the IT administrator for your organization. You want to ensure that you can trace all remote access sessions to a specific user. You configure the VPN device to capture the following information for all remote access connections:

- source and destination IP address;
- user ID;
- machine name;
- time stamp; and
- user actions during the remote session.

This lets you trace these actions to a specific user.

Mapping

- NIST SP 800-53R4: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12
- NIST SP 800-171: 3.3.2
- CIS: 16.8,16.9
- CSF: DE.CM-1,DE.CM-3,DE.CM-7

NIST SP 800-171R2 Related Security Requirement: Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

NIST SP 800-171R2 Related Discussion: This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of Voice over Internet Protocol (VoIP).

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing system audit logging].

Testing Assessment Notes:

Maturity Level 2

Capability C008: Perform auditing

Practice AU.2.042: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

Discussion: [DRAFT NIST SP 800-171 R2]: An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

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

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

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

CMMC Clarification: You should ensure that the system creates and retains audit logs. The logs should contain enough information to identify and investigate unlawful or unauthorized system activity. You select the events that require auditing. Also, you determine the information to record in the audit logs about those events.

Example

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

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

Mapping

- NIST SP 800-53R4: AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12
- NIST SP 800-171: 3.3.1
- CIS: 6.2
- CSF: DE.CM-1,DE.CM-3,DE.CM-7

NIST SP 800-171R2 Related Security Requirement: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

NIST SP 800-171R2 Related Discussion: An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloudbased architectures. Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred). Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual

identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making.

Assessment

Assessment Objective(s): Determine if:

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

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

3.3.1[c] audit records are created (generated).

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

3.3.1[e] retention requirements for audit records are defined.

3.3.1[f] audit records are retained as defined.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing system audit logging].

Testing Assessment Notes:

Maturity Level 2

Capability C008: Perform auditing

Practice AU.2.043: Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Discussion: [DRAFT NIST SP 800-171 R2]: Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

CMMC Clarification: Some organizations have many machines. It is good practice to setup each machine to synchronize its time with a central time server. This ensures that all machines are recording audit logs using the same time source. This is important when you review audit logs for suspicious activity. You need to review events from multiple machines. This can be a difficult task if the time is not synchronized for all machines. To use the same time source, you can synchronize machines to a network device or directory service. Also, you can configure machines manually to use the same time servers on the internet.

Example

You are setting up several new computers on your company's network. They are not setup on a domain. You update the time settings on each machine to use the same authoritative time server on the internet. If you have to review audit logs, all your machines will have synchronized time. This helps you investigate a potential incident.

Mapping

- NIST SP 800-53R4: AU-8, AU-8(1)
- NIST SP 800-171: 3.3.7
- CIS: 6.1
- CSF: PR.PT-1

NIST SP 800-171R2 Related Security Requirement: Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

NIST SP 800-171R2 Related Discussion: Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time

measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network. See [IETF 5905].

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

AU: Audit and Accountability C010:AU.2.044

Maturity Level 2

Capability C010: Review and manage audit logs

Practice AU.2.044: Review audit logs.

Discussion: [CMMC]: Reviewing audit logs is a common control in information security. Organizations have the flexibility to determine which logs and specific events to review. The level of audit log review should be determined based on a risk assessment or similar activity.

CMMC Clarification: You should ensure that your organization reviews its audit logs. Logs should be checked regularly, organizations with small environments may be able to do this manually. The process of reviewing audit logs varies by organization. The intent of this practice is to become familiar with the logs being automatically created on the systems present in your organization and identify key events in the logs that might indicate malicious activity. Larger organizations may need automation to complete this task with success.

Example

You are the administrator for a company with a small IT environment. You know the importance of reviewing audit logs. Every week you log on to the Windows server as an admin user, open the Event Viewer and check for signs that the log files have been altered: Windows event ID 104 – Event Log was Cleared, event ID 1102 – Audit Log was Cleared), event ID 4719 – System audit policy was changed. Look for login and new user created events: Windows event IDs 4624 (failure) and 4625 (success)) and event IDs 4728, 4732 and 4756 – User added to Privileged Group.

Mapping

- NIST SP 800-53R4: AU-6
- NIST SP 800-171:
- CIS: 6.7
- CSF: PR.PT-1

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C007: Define audit requirements

Practice AU.3.045: Review and update logged events.

Discussion: [DRAFT NIST SP 800-171 R2]: Periodically re-evaluate which events are logged and which events should be added, modified, or deleted. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

CMMC Clarification: Organizations should periodically review logged events that identify possible security incidents, and the organization should update the list of events that need to be logged as necessary. Non-security events that should have logging requirements reviewed include 1) logging all installed software on endpoints to identify license irregularities or 2) logging connections to a VPN server or load balancer to manage capacity and quality of service.

Example

You are in charge of IT operations for your organization. You are responsible for identifying and documenting which events are relevant to the security of your organization's systems. Your organization has decided that this list of security revelant events should be updated annually or when a new security threats or events have been identified requiring additional events to be logged and reviewed.

You perform your annual review of events to log. The list includes events your organization reviewed and determined to be important for security. This list started as the list of recommended events given by the manufacturers of your operating systems / devices but has grown from experience operating the security of your environment and learned additional best practices from security training and knowledge sharing with peers.

There is a security incident at your organization. Working with the security officer, a forensics review shows the logs appears to have been deleted by a remote user, and you notice that remote sessions are not currently logged. You update the list of events to include all VPN sessions.

Mapping

- NIST SP 800-53R4: AU-2(3)
- NIST SP 800-171: 3.3.3
- CIS: 6.7
- CSF:

NIST SP 800-171R2 Related Security Requirement: Review and update logged events.

NIST SP 800-171R2 Related Discussion: The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C007: Define audit requirements

Practice AU.3.046: Alert in the event of an audit logging process failure.

Discussion: [DRAFT NIST SP 800-171 R2]: Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

CMMC Clarification: Audit logging keeps track of activities occurring on the network, servers, user workstations and other components of the overall system. These logs must always be available and functional. The organization's designated security personnel (e.g., system administrator and security officer) need to be aware when the audit log process fails or becomes unavailable. Automated notifications need to be sent to the organization's designated security personnel to immediately take appropriate action. If security personnel are unaware of the audit logging process failure, then they will be unaware of any suspicious activity occurring at that time. Your response to an audit logging process failure should account for the extent of the failure (e.g., a single component's audit logging versus failure of the centralized logging solution), the risks involved in this loss of audit logging, and other factors (e.g., possibility an adversary could have caused the audit logging process failure).

Example

You are in charge of IT operations for your organization. Your responsibilities include management of the audit logging process. One of the logging mechanisms failed, but you had configured the system to notify the designated security personnel that a problem with the auditing system occurred. After verifying the alert, you restart the logging mechanism and verify that it is now logging.

Mapping

- NIST SP 800-53R4: AU-5
- NIST SP 800-171: 3.3.4
- CIS: 6.7
- CSF:

NIST SP 800-171R2 Related Security Requirement: Alert in the event of an audit logging process failure.

NIST SP 800-171R2 Related Discussion: Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

AU: Audit and Accountability C008:AU.3.048

Maturity Level 3

Capability C008: Perform auditing

Practice AU.3.048: Collect audit information (e.g., logs) into one or more central repositories.

Discussion: [CMMC]: Aggregate and store audit logs in a central location. Central repositories enable analysis by storing audit record content needed for analysis in a common location and format. Storing audit logs in central repositories also protects audit information. The repository has the available infrastructure, capacity, and protection mechanisms to meet the organization's audit requirements. Policy and local laws may place requirements on the location and structure of the repositories.

CMMC Clarification: Aggregate and store audit logs in a centralized location or locations within the organization. Storing audit logs in a centralized location supports orchestration, automation, correlation, and analysis activities by enabling a full picture of the audit logs, and can support automated analysis capabilities including correlation of events across the enterprise. Ensure that the central repository has the appropriate infrastructure, including protection mechanisms, and the capacity level to meet the logging requirements of the organization.

Example

You are in charge of IT operations in your organization. Your responsibilities include reviewing audit logs. You consolidate all audit logs in a common format and into a centralized logging infrastructure that may consist of one or more servers. By doing this, you enable centralized analysis of your audit logs. This increases situational awareness across your network. In addition, you are able to better protect your audit logs by storing them in one centralized location.

Mapping

- NIST SP 800-53R4: AU-6(4)
- NIST SP 800-171:
- CIS: 6.5
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C009: Identify and protect audit information

Practice AU.3.049: Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Discussion: [DRAFT NIST SP 800-171 R2]: Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.

CMMC Clarification: Audit information is a critical record of what events occurred, the source of the events, and the outcomes of the events; this information needs to be protected. This protection starts with ensuring proper configuration of logging to ensure proper space for the needed log retention. The logs must also be properly secured so that the information may not be modified or deleted, either intentionally or unintentionally. Only those with a legitimate need-to-know should have access to audit information, whether that information is being accessed directly from logs or from audit tools.

Example

You are in charge of IT operations in your organization. Your responsibilities include protecting audit information and audit logging tools. You protect the audit information by having audit log events forwarded to a central server and by restricting the local audit logs to only be viewable by the system administrators. Centralized audit information is protected from deletion or alteration and only approved individuals can view the information in the audit tool. The central audit information server is backed up daily with those backups being encrypted and sent offsite where they are physically secured by a third-party.

Mapping

- NIST SP 800-53R4: AU-6(7), AU-9
- NIST SP 800-171: 3.3.8
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

NIST SP 800-171R2 Related Discussion: Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.

Assessment

Assessment Objective(s): Determine if:

3.3.8[a] audit information is protected from unauthorized access.

3.3.8[b] audit information is protected from unauthorized modification.

3.3.8[c] audit information is protected from unauthorized deletion.

3.3.8[d] audit logging tools are protected from unauthorized access.

3.3.8[e] audit logging tools are protected from unauthorized modification.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing audit information protection].

Testing Assessment Notes:

Maturity Level 3

Capability C009: Identify and protect audit information

Practice AU.3.050: Limit management of audit logging functionality to a subset of privileged users.

Discussion: [DRAFT NIST SP 800-171 R2]: Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

CMMC Clarification: Organizations should restrict access to audit logging functions to a limited number of privileged users that can modify audit logs and audit settings. There are three classes of users: general users, privileged users, and audit managers. General users should not be granted permissions to perform audit management. All audit managers should come from the set of privileged users, but only a small subset of privileged users will be given audit management responsibilities. Functions performed by privileged users must be distinctly separate from the functions performed by users who have audit-related responsibilities to reduce the potential of fraudulent activities by privileged users not being detected or reported. Example

You are in charge of IT operations in your organization. You are responsible for the administration of the infrastructure, but you are not an audit manager and cannot review audit logs, delete audit logs, or modify audit log settings. Full control of audit logging functions has been given to the security auditors, and they are able to review logs and modify audit log settings. This separation of system administration duties from audit logging management is necessary to prevent possible log file tampering.

Mapping

- NIST SP 800-53R4: AU-6(7), AU-9(4)
- NIST SP 800-171: 3.3.9
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Limit management of audit logging functionality to a subset of privileged users.

NIST SP 800-171R2 Related Discussion: Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C010: Review and manage audit logs

Practice AU.3.051: Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Discussion: [DRAFT NIST SP 800-171 R2]: Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

CMMC Clarification: Organizations must review, analyze, and report audit records to help detect and respond to security incidents in a timely manner for the purpose of investigation and corrective actions. Collection of audit logs into one or more central repositories (per AM.3.048) facilitates correlated review. Small organizations may be able to accomplish this manually. Larger organizations will use an automated system for analysis that does correlation of log information across the entire enterprise and supports the use of centralized intel feeds. By centralizing intel feeds, subscription costs should be reduced and the effectiveness of the analysis should be increased. Some organizations may want to orchestrate the entire analysis process which includes the use of APIs for collection, correlation, and the automation of responses based on programed rulesets.

Example 1

You are in charge of IT operations in your organization. You are responsible for assisting in the investigation of a possible incident. You review the event log for suspicious activity, e.g., a user logged on at an unusual time of day. In order to analyze the data, you use an automated tool to collect and analyze the audit log data, and perform queries to generate a detailed report. Once the connection is made between the individual and the incident, corrective actions are taken.

Example 2

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

Mapping

- NIST SP 800-53R4: AU-6(3)
- NIST SP 800-171: 3.3.5
- CIS: 6.6,6.7
- CSF: DE.AE-3

NIST SP 800-171R2 Related Security Requirement: Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

NIST SP 800-171R2 Related Discussion: Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C010: Review and manage audit logs

Practice AU.3.052: Provide audit record reduction and report generation to support ondemand analysis and reporting.

Discussion: [DRAFT NIST SP 800-171 R2]: Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

CMMC Clarification: Raw audit log data is difficult to review, analyze, and report because of the volume of data. Audit record reduction is an automated process that interprets raw audit log data and extracts meaningful and relevant information without altering the original logs. An example of log reduction for files to be analyzed would be the removal of details associated with nightly backups. Report generation on reduced log information allows you to create succinct customized reports without the need to burden the reader with unimportant information. In addition, the security relevant audit information must be made available to personnel ondemand for immediate review, analysis, reporting, and event investigation support. Peforming audit log reduction and providing on-demand reports may allow the analyst to take mitigating action before the adversary completes their malicious actions.

Example

You are in charge of IT operations in your organization. You are responsible for providing audit record reduction and report generation capability to effectively extract security relevant information. You either purchase or develop a capability that will collect and analyze data for signs of anomalies. The system then extracts security relevant data to provide a reduced, concise, and comprehensive view for further analysis to identify potentially malicious activity on your network. In addition to creating on-demand data sets for analysis, you create customized reports explaining the contents of the data set.

Mapping

- NIST SP 800-53R4: AU-7
- NIST SP 800-171: 3.3.6
- CIS:
- CSF: RS.AN-3

NIST SP 800-171R2 Related Security Requirement: Provide audit record reduction and report generation to support on-demand analysis and reporting.

NIST SP 800-171R2 Related Discussion: Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to

analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 4

Capability C010: Review and manage audit logs

Practice AU.4.053: Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.

Discussion: [CMMC]: Adversary activity typically leaves indications in audit logs. Patterns and signatures from previously seen adversary activity or malicious software are shared and can be used in automated analysis. Organizations can define thresholds for the level and definition of suspicious activity on which to take an action. The automated activity can be distributed or centralized.

CMMC Clarification: Speed of response can be critical in stopping a cyber attack and limiting exposure to the attack. The speed of response is improved when log source platforms automatically and immediately identify indicators for which immediate action is required and authorized to be taken automatically. Some logging platforms will not support automated analysis and action. In those cases, the immediate analysis occurs at the centralized log collection server (see practice AU.3.048).

The analysis would look for specific log entry text or data element values in cases where there is certainty that an action should and can occur immediately, as defined by the organization. Actions may range from notifications to blocks. The actions must be automatic but need not be comprehensive in stopping the threat.

Example

Upon seeing a specific text string in a log on the corporate CUI database server indicating that a large query had been requested, an alert is generated to notify the security operations center (SOC) of the log event. The SOC processes the alert automatically and a full report is generated and a window pops up for the SOC member responsible for the CUI database as well as the overall SOC lead.

In a more clear and critical case, where evidence of compromise is conclusive and decisive and response is already authorized by senior management, the action may be to cut off the server from some connected systems or to even shut down the server to prevent further exposure or data exfiltration. The clear evidence may have been provided by external shared indicators of a cyber incident at a peer organization for which early warning signs have been identified.

Mapping

- NIST SP 800-53R4: SI-4(2)
- NIST SP 800-171:
- CIS: 6.6
- CSF: DE.AE-3

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C010: Review and manage audit logs

Practice AU.4.054: Review audit information for broad activity in addition to per-machine activity.

Discussion: [CMMC]: The full scope of adversary activity may not be apparent from analyzing a single machine. A broad perspective is necessary for full cybersecurity situational awareness. Activity might be reviewed across multiple machines, an enclave, or an entire enterprise. This will require audit logs collated with the same scope as the analysis.

CMMC Clarification: Examining audit logs for system-specific indicators provides an important "point-defense" ability for a specific system (see practice AU.4.053). Comparing log information across multiple disparate systems allows for a holistic and time-correlated approach to detect cyber attack actions that would not constitute a threat indicator or generate any action when identified on any single system. Some of these attacks may be subtle or infrequent, while others just comprise a large number of machines. This practice requires that a system perspective be used to look for these subtle and distributed (in both logical space and time) indicators and to act upon detecting them in line with other auditing practices. The definition and scope of the system perspective will vary as the size of the organization or enclave changes. For very small installations, broad activity may only mean more than one system.

Example 1

You are working your shift in the security operations center (SOC) when you are alerted to a trend that has appeared in logs from across the company networks. The centralized log collection server has identified minor indicators that show periodic increases in failed login attempts across most of the corporate data servers. While the number of failed attempts did not cross the threshold for account locking, together they passed the 24-hour moving window for failed login attempts, having exceeded the average of such attempts by 1000%. You obtain a list of all account names for which access failed and see that four accounts have had extremely high failure counts. You initiate a log query to identify the IP addresses of the systems that attempted to access these four accounts over the past 10 days and notify the threat hunting team of the analysis results.

Example 2

As part of the security operations center (SOC) standard operating procedures (SOP), you execute a run of a log analysis tool on the system-wide audit log looking for pre-defined indicators of broad security-relevant activity. The analysis tool notifies you that afternormal-work-hours, failed login attempts are occurring across a large number of machines resulting in locked accounts across the system. On a machine-by-machine basis a locked account does not warrant any escalation but across multiple systems this indicates a potential denial of service attack to cause a significant impact on workforce productivity at the start of the next workday.

Mapping

- NIST SP 800-53R4: RA-5(6), RA-5(8), RA-5(10)
- NIST SP 800-171:

- CIS:
- CSF: PR.PT-1

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C008: Perform auditing

Practice AU.5.055: Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.

Discussion: [CMMC]: Practice AU.2.042 required the creation and retention of audit logs. Audit logs are essential to cybersecurity awareness and incident response. This practice requires organizations to proactively determine if any assets that should be creating audit logs are not generating the required logs.

CMMC Clarification: Robust audit logging is critical in defending against cyber attacks and preventing future attacks since logs are a common starting point for incident response and a core element in post-attack cyber forensics. A cyber attacker may try to disrupt logging at the start of an attack, making the absence of audit logging an initial indicator of a potential attack. Even if the audit logging failure occurred from benign causes, restoring the logging is needed to maintain a secure posture.

Identifying assets that are reporting logs and comparing against the inventory of assets expected to provide audit logs provides the set of assets for which audit remediation is needed. It is important that the logging requirements for each asset, which may include many logs to be collected, are documented and compared to the set of received logs. Any discrepancies will start an investigation and remediation process.

Example

You are working your shift in the security operations center (SOC) when one of your hourly scanning scripts indicates that a data server is not providing logs to the central log collection server. The data server is on the list of assets for which a log is required. You send a notification to the administrator for the server to investigate and turn logging on, and copy the company threat hunting team as well.

Mapping

- NIST SP 800-53R4: AU-12
- NIST SP 800-171:
- CIS: 6.2
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C011: Conduct security awareness activities

Practice AT.2.056: Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

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

CMMC Clarification: Awareness training focuses user attention on security. You can use several techniques to do this:

- instructor or online training;
- security awareness campaigns; and
- posters and email advisories and notices to employees.

There is an important distinction between awareness training and role-based training. Awareness training provides general security training to influence user behavior. Rolebased training focuses on the knowledge, skills, and abilities needed to complete a specific job.

Example

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

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

You encourage everyone to not click on attachments or links in a suspicious email. You tell employees to forward such a message immediately to their IT security administrator. You download free security awareness posters to hang in the office. Also, you send regular emails and tips to all employees. This ensures that your message is not forgotten over time.

Mapping

- NIST SP 800-53R4: AT-2, AT-3
- NIST SP 800-171: 3.2.1
- CIS: 17.3
- CSF: PR.AT-1,PR.AT-2,PR.AT-3,PR.AT-4,PR.AT-5

NIST SP 800-171R2 Related Security Requirement: Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

NIST SP 800-171R2 Related Discussion: Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

Assessment

Assessment Objective(s): Determine if:

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

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C012: Conduct training

Practice AT.2.057: Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

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

CMMC Clarification: Training imparts skills and knowledge. It enables staff to perform a specific resilience function. Training programs identify cybersecurity skill gaps within your organization. Then, the programs train users on their specific cybersecurity roles and responsibilities.

There is an important distinction between awareness training and role-based training. Awareness training provides general security training to influence user behavior. Rolebased training focuses on the knowledge, skills, and abilities needed to complete a specific job.

Example

Your company upgraded the firewall to a newer, more advanced system. Your company identified you as an employee who needs training on the device. This will enable you to use it effectively. Your company considered this when it planned for the upgrade. It made training funds available as part of the upgrade project.

Mapping

- NIST SP 800-53R4: AT-2, AT-3
- NIST SP 800-171: 3.2.2
- CIS: 17.5,17.6,17.7,17.8,17.9
- CSF: PR.AT-1,PR.AT-2,PR.AT-3,PR.AT-4,PR.AT-5

NIST SP 800-171R2 Related Security Requirement: Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

NIST SP 800-171R2 Related Discussion: Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities for security awareness training; personnel with information security respon

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C011: Conduct security awareness activities

Practice AT.3.058: Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Discussion: [DRAFT NIST SP 800-171 R2]: Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

CMMC Clarification: An insider threat is an employee or contractor that is authorized for computing or network activities, but conducts malicious activity with that access. The insider threat security awareness training focuses on recognizing employee behaviors and characteristics that might be indicators of an insider threat and knowing the guidelines and procedures on how to handle and report it. Training for managers will provide guidance on observing team members to identify all potential threat indicators, while training for general employees will be slightly different and provide guidance for focusing on a smaller number of indicators. While all the indicators are important, general employees may be on different teams and knowledge of their job dissatisfaction or requests for information not required for adequate job performance is unknown. In other words, it is important to tailor the training for specific roles rather than having the same training program for everyone.

Example

You are responsible for training all employees on the awareness of high risk behaviors that can indicate a potential insider threat, so you add the following example to the training package: The organization has created a baseline of normal behavior for work schedules. One employee's normal work schedule is 8:00 AM-5:00 PM, but another employee noticed that the employee has been working until 9:00 PM every day even though no special projects have been assigned and no short time frame deliverables have been identified. The observing employee reports the unjustified abnormal work schedule using the established guidelines of the organization.

Mapping

- NIST SP 800-53R4: AT-2(2)
- NIST SP 800-171: 3.2.3
- CIS:
- CSF: ID.RA-3

NIST SP 800-171R2 Related Security Requirement: Provide security awareness training on recognizing and reporting potential indicators of insider threat.

NIST SP 800-171R2 Related Discussion: Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

Assessment

Assessment Objective(s): Determine if:

3.2.3[a] potential indicators associated with insider threats are identified.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms managing insider threat training].

Testing Assessment Notes:

Maturity Level 4

Capability C011: Conduct security awareness activities

Practice AT.4.059: Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the

Discussion: [DRAFT NIST SP 800-171B]: One of the most effective ways to detect APT activities and to reduce the effectiveness of those activities is to provide specific awareness training for individuals. A well-trained and security aware workforce provides another organizational safeguard that can be employed as part of a defense- in-depth strategy to protect organizations against malicious code injections via email or the web applications. Threat awareness training includes educating individuals on the various ways APTs can infiltrate into organizations including through websites, emails, advertisement pop-ups, articles, and social engineering. Training can include techniques for recognizing suspicious emails, the use of removable systems in nonsecure settings, and the potential targeting of individuals by adversaries outside the workplace. Awareness training is assessed and updated periodically to ensure that the training is relevant and effective, particularly with respect to the threat since it is constantly, and often rapidly, evolving.

CMMC Clarification: This practice requires that awareness training specifically include tactics and indicators used by advanced cyber threat actors. The intent is to go beyond the basic cyber security awareness training elements such as password management and good cyber hygiene and to broaden awareness for more advanced attack techniques.

Example

You manage cyber awareness training for the company. You are notified by a cybersecurity team member that a well-known cyber-attack team known as Fancy Bear has recently gone after peer organizations. The team member shares that one of their most common first steps is to look up employees via publicly available information sources, such as social media and corporate connection applications, and then craft well-targeted phishing attacks against software developers that invites them to a free conference in an overseas location. You quickly create and disseminate materials to sensitize corporate software developers to email phishing attacks and provide specific information, including examples, of prior Fancy Bear phishing emails as well as “friend” and “connection” requests. You also include the updates in the standard awareness training for the entire organization.

Mapping

- NIST SP 800-53R4: AT-2, AT-2(3), AT-2(4), AT-2(6), AT-2(7)
- NIST SP 800-171:
- CIS: 17.1,17.2,17.4
- CSF: PR.AT-1,PR.AT-2,PR.AT-3,PR.AT-4,PR.AT-5

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C011: Conduct security awareness activities

Practice AT.4.060: Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training.

Discussion: [DRAFT NIST SP 800-171B (MODIFIED)]: Awareness training is most effective when it is complemented by practical exercises tailored to the tactics, techniques, and procedures (TTPs) of the threat. Examples of practical exercises include no-notice social engineering attempts to gain unauthorized access, collect information, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Rapid feedback is essential to reinforce desired user behavior. Training results, especially failures of personnel in critical roles, can be indicative of a potential serious problem. [Modified only to remove requirement to notify supervisors from NIST SP 800-171B 3.2.2e].

CMMC Clarification: This practice increases the effectiveness of security awareness and training by including exercises that directly related to real-world threats. In addition, the intent of the requirement for feedback is to ensure that the organization is proactive in seeking to measure the value being achieved by these exercises.

Example

You manage cyber awareness training for the company. You have been notified by the company cybersecurity team that a well-known cyber-attack team known as “Fancy Bear” has recently gone after peer organizations. You create a well-targeted phishing attack that appears to come from an external source aimed at company employees in the software development branch. When an employee clicks on a “bad” link, a notice is sent by the receiving server to corporate security and a message is automatically generated once the exercise ends to notify the employee that they should not have clicked the link and providing the clues that would have allowed them to identify the phishing attack.

In an effort to “raise their game” in the speed and relevance of their phishing prevention program, you work with the IT branch to create a process that takes actual “same day” phishing attacks that were identified by email defenses. The first step is to neutralize the emails by replacing attachments with corporate “Trojan horse” files and external links with a corporate phishing remote server link. Then the neutered but authentic phishing attack email is sent to the previous set of corporate addresses. Doing this allows you to train staff against actual threats at a faster pace and saves on the overhead of creating a realisticlooking phishing message.

Mapping

- NIST SP 800-53R4: AT-2(1), AT-2(8)
- NIST SP 800-171:
- CIS: 17.1,17.2,17.4
- CSF: PR.AT-1,PR.AT-2,PR.AT-3,PR.AT-4,PR.AT-5

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C013: Establish configuration baselines

Practice CM.2.061: Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement establishes and maintains baseline configurations for systems and system components including for system communications and connectivity. Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration.

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

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

Build and configure systems from a known, secure, and approved configuration baseline. This includes:

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

An effective cybersecurity program depends on system and component configuration and management.

Example

You are in charge of upgrading the computer operating systems of your office’s 10 machines. You research how to setup and configure a machine with the least functionality and highest security. The

setup must allow users to do their tasks. You document this configuration. Then, you apply it to the other nine machines. You understand the baseline configuration of every machine. This helps when you need to install new patches, software, or make changes.

CMMC Clarification:

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171: 3.4.1
- CIS: 1.4,1.5,2.1,2.4,5.1
- CSF: ID.AM-1,ID.AM-2,PR.DS-3,PR.DS-7,PR.IP-1,DE.AE-1

NIST SP 800-171R2 Related Security Requirement: Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

NIST SP 800-171R2 Related Discussion: Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

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

Assessment

Assessment Objective(s): Determine if:

3.4.1[a] a baseline configuration is established.

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

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

3.4.1[d] a system inventory is established.

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsib

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organization

Testing Assessment Notes:

Maturity Level 2

Capability C013: Establish configuration baselines

Practice CM.2.062: Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Discussion: [DRAFT NIST SP 800-171 R2]: Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components. However, doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component.

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

CMMC Clarification: You should customize organizational systems. To do this, remove non-essential applications and disable services not needed. Systems come with many unnecessary applications and settings enabled by default. Disable unnecessary software and services. These include unused ports and protocols. Leave only the fewest capabilities necessary for the systems to operate effectively.

Example

You know that systems often include unnecessary software and services enabled by default. You deploy new servers in your organization's IT environment. Before you do so, you review each system's role and minimum required capabilities. You remove software that is not needed. You disable unused ports and services. You leave only the essential capabilities enabled for the system to function in its role.

Mapping

- NIST SP 800-53R4: CM-7
- NIST SP 800-171: 3.4.6
- CIS:
- CSF: PR.IP-1,PR.PT-3

NIST SP 800-171R2 Related Security Requirement: Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

NIST SP 800-171R2 Related Discussion: Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components. However, doing so increases risk over limiting the

services provided by any one component. Where feasible, organizations limit component functionality to a single function per component.

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Assessment

Assessment Objective(s): Determine if:

3.4.6[a] essential system capabilities are defined based on the principle of least functionality.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C013: Establish configuration baselines

Practice CM.2.063: Control and monitor user-installed software.

Discussion: [DRAFT NIST SP 800-171 R2]: Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved "app stores." Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

CMMC Clarification: You should limit installed software to items that the organization approved. Users will install software that creates unnecessary risk. This risk applies both to the machine and to the larger operating environment. You should control the software users can install. You should put in place policies and technical controls that can reduce risk to the organization.

Example

You are the IT administrator for your company. A user calls you for help installing a software package. He keeps receiving a message asking for a password. The user receives the message because he does not have permission to install the software. You explain the organization's policy. It prohibits users from installing software without approval. When you set up workstations for users, you do not provide administrative privileges. You make an exception only if a user needs administrative access to do his job. After the call, you redistribute the policy to all users ensuring everyone in the organization is aware of the restrictions.

Mapping

- NIST SP 800-53R4: CM-11
- NIST SP 800-171: 3.4.9
- CIS: 2.1,2.2,2.6
- CSF: DE.CM-3

NIST SP 800-171R2 Related Security Requirement: Control and monitor user-installed software.

NIST SP 800-171R2 Related Discussion: Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved "app stores." Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or

provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

Assessment

Assessment Objective(s): Determine if:

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

3.4.9[b] installation of software by users is controlled based on the established policy.

3.4.9[c] installation of software by users is monitored.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C014: Perform configuration and change management

Practice CM.2.064: Establish and enforce security configuration settings for information technology products employed in organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

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

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

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

CMMC Clarification: Security-related configuration settings should be customized and included as part of an organization's baseline configurations for all information systems. These configuration settings should satisfy the organization's security requirements and changes or deviations to the security settings should be documented. Organizations should document the Securityrelated configuration settings and apply them to all systems once tested and approved. The configuration settings should reflect the most restrictive settings that are appropriate for the system. This ensures that information security is an integral part of an organization's configuration management process.

Example

You are in charge of establishing baseline configurations for your organization's systems. As part of this, you document the most restrictive settings that still allow the system to function as required and apply this configuration to all applicable systems. This secure configuration, also known as a system lockdown,

blocks unapproved applications from running on the system. The lockdown configuration aligns with your organization's security requirements.

Mapping

- NIST SP 800-53R4: CM-2, CM-6, CM-8, CM-8(1)
- NIST SP 800-171: 3.4.2
- CIS: 1.4,1.5,2.1,2.4,5.1
- CSF: ID.AM-1,ID.AM-2,PR.DS-3,PR.DS-7,PR.IP-1,DE.AE-1

NIST SP 800-171R2 Related Security Requirement: Establish and enforce security configuration settings for information technology products employed in organizational systems.

NIST SP 800-171R2 Related Discussion: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

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

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

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings; proc

Testing Assessment Notes:

Maturity Level 2

Capability C014: Perform configuration and change management

Practice CM.2.065: Track, review, approve, or disapprove, and log changes to organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

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

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

CMMC Clarification: You should track, review, and approve changes before committing to production. Changes to computing environments can create unintended and unforeseen issues. They can affect the security and availability of the systems. Organizations should hold regular meetings about changes. Relevant experts should review and approve proposed changes. They should discuss potential impacts, before the organization puts the changes in place. Relevant items include changes to the physical environment and to the system hosted within it.

Example

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

Mapping

- NIST SP 800-53R4: CM-3
- NIST SP 800-171: 3.4.3
- CIS:
- CSF: PR.IP-1,PR.IP-3

NIST SP 800-171R2 Related Security Requirement: Track, review, approve or disapprove, and log changes to organizational systems.

NIST SP 800-171R2 Related Discussion: Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

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

Assessment

Assessment Objective(s): Determine if:

3.4.3[a] changes to the system are tracked.

3.4.3[b] changes to the system are reviewed.

3.4.3[c] changes to the system are approved or disapproved.

3.4.3[d] changes to the system are logged.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C014: Perform configuration and change management

Practice CM.2.066: Analyze the security impact of changes prior to implementation.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

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

CMMC Clarification: You should analyze the potential security impact of changes before implementing them. Changes to complex environments can cause unforeseen problems to systems and environments. You should perform an analysis that focuses on the security impact of changes. This can uncover potential problems before you implement the change. By doing so, you can help mitigate unforeseen problems.

Example

Someone requests major changes to the system and environment. You must complete a process with several steps before you can put the change in place. You document a detailed plan which includes the security impact of the change. A SME who did not submit the change reviews the plan. That SME tries to identify security-related issues that the change may cause. Then, they document or correct the potential issues. Also, they submit the updated change plan to your organization's change control board.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171: 3.4.4
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Analyze the security impact of changes prior to implementation.

NIST SP 800-171R2 Related Discussion: Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the

implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

Assessment

Assessment Objective(s): Determine if the security impact of changes to the system is analyzed prior to implementation.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C014: Perform configuration and change management

Practice CM.3.067: Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries. Access restrictions include physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during certain specified times). In addition to security concerns, commonly-accepted due diligence for configuration management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration.

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

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

Example 1

You are in charge of IT operations in your organization responsible for configuration management. You need to add an additional network storage appliance to a server farm. However, all of your organization's servers have been consolidated into a single data center that has locked doors. To gain access to that data center, you request and are granted a key card which allows you to enter the data center and modify the hardware configuration.

Example 2

You are responsible for patching your organization's software as soon as new versions are released or when emergency patching is required. You configure the patch management system to push patches to all endpoints in the enterprise as soon as a patch or update is available, has been confirmed to have been received from the proper source, and has been validated.

Mapping

- NIST SP 800-53R4: CM-5
- NIST SP 800-171: 3.4.5
- CIS: 2.5,2.7,2.8,2.9,4.3,11.1,11.3,11.7
- CSF: PR.IP-1

NIST SP 800-171R2 Related Security Requirement: Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

NIST SP 800-171R2 Related Discussion: Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries.

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

Assessment

Assessment Objective(s): Determine if:

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

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

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

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

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

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

3.4.5[g] logical access restrictions associated with changes to the system are approved.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C014: Perform configuration and change management

Practice CM.3.068: Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Discussion: [DRAFT NIST SP 800-171 R2]: Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, FTP, and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.

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

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

Example

You are responsible for purchasing new endpoint hardware, installing organizationally required software to the hardware, and configuring the endpoint in accordance with the organization's policy, The organization has a system imaging capability that loads all necessary software, but it does not remove unnecessary services, eliminate the use of certain protocols, or close unused ports. After imaging the systems you close all ports and block the use of all protocols except the following:

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

The use of any other ports or protocols are allowed by exception only.

Mapping

- NIST SP 800-53R4: CM-7(1), CM-7(2)
- NIST SP 800-171: 3.4.7
- CIS: 9.2,9.4,12.4
- CSF: PR.IP-1,PR.PT-3

NIST SP 800-171R2 Related Security Requirement: Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

NIST SP 800-171R2 Related Discussion: Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.

Assessment

Assessment Objective(s): Determine if:

3.4.7[a] essential programs are defined.

3.4.7[b] the use of nonessential programs is defined.

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

3.4.7[d] essential functions are defined.

3.4.7[e] the use of nonessential functions is defined.

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

3.4.7[g] essential ports are defined.

3.4.7[h] the use of nonessential ports is defined.

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

3.4.7[j] essential protocols are defined.

3.4.7[k] the use of nonessential protocols is defined.

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

3.4.7[m] essential services are defined.

3.4.7[n] the use of nonessential services is defined.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services; mechanisms implementing review and handling of nonessential programs, functions, ports, protocols, or services; organizatio

Testing Assessment Notes:

Maturity Level 3

Capability C014: Perform configuration and change management

Practice CM.3.069: Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Discussion: [DRAFT NIST SP 800-171 R2]: The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

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

Example

You are in charge of managing the IT infrastructure within your organization. To provide better protection for your company you have decided to take a whitelist approach. With additional research you identify a capability within the latest operating system that can control executables, scripts, libraries, or application installers run in your environment. To ensure success you begin by authorizing digitally signed executables. Once deployed you then plan to evaluate and deploy whitelisting for software libraries and scripts.

Mapping

- NIST SP 800-53R4: CM-7(4), CM-7(5)
- NIST SP 800-171: 3.4.8
- CIS: 2.1,2.2,2.6,2.7,2.8,2.9
- CSF:

NIST SP 800-171R2 Related Security Requirement: Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

NIST SP 800-171R2 Related Discussion: The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for

example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 4

Capability C014: Perform configuration and change management

Practice CM.4.073: Employ application whitelisting and an application vetting process for systems identified by the organization.

Discussion: [DRAFT NIST SP 800-171 R2 (MODIFIED)]: The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup. This practices requires the use of application whitelisting where feasible. NIST SP 800-167 provides guidance on application whitelisting.

CMMC Clarification: The organization has a procedure to validate systems used for processing CUI information and to identify the applications required for CUI processing. The procedure includes the steps a new application must go through to check it is not malicious and there is a business requirement for the application before it is added to the whitelist. The organization has configured their systems (e.g., desktop, laptop, tablet) to check an application has been approved for use (whitelisted) before the application can run. All unapproved applications are, by default blocked from running on the organization's systems. See practice RM.5.152 for more information on handling non-whitelisted software. This is a CMMC modificationof NIST SP 800-171r1 3.4.8.

Example 1

You are responsible for system security at your organization. An employee asks you to approve a data visualization application they want to use to develop charts in their final report to the sponsor. After you confirm with the project manager that the application is required, you run a script to calculate the MD5 hash value for the executable and submit it to virustotal.com for validation. After confirming the application is safe you add the application to the whitelist.

Example 2

You are responsible for system security at your organization. An employee asks you to whitelist an application found through an Internet search. You download a copy of the file and submit it to virustotal.com. You determine that it is malicious. You delete all copies of the application from all of your organizations's computers and do not add it to the organization's whitelist.

Mapping

- NIST SP 800-53R4: CM-7(4), CM-7(5)
- NIST SP 800-171: 3.4.8
- CIS: 2.1,2.2,2.6,2.7,2.8,2.9
- CSF: PR.PT-3

NIST SP 800-171R2 Related Security Requirement: Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

NIST SP 800-171R2 Related Discussion: The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 5

Capability C014: Perform configuration and change management

Practice CM.5.074: Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).

Discussion: [DRAFT NIST SP 800-171B (MODIFIED)]: Verifying the integrity of the organization's security critical or essential software is an important capability as corrupted software is the primary attack vector used by adversaries to undermine or disrupt the proper functioning of organizational systems. There are many ways to verify software integrity and correctness throughout the system development life cycle. Root of trust mechanisms such as secure boot and trusted platform modules verify that only trusted code is executed during boot processes. This capability helps system components protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying boot firmware. Formal verification involves proving that a software program satisfies some formal property or set of properties. The nature of such formal verification is generally time consuming and not employed for most commercial operating systems and applications. Therefore, it would likely only be applied to some very limited uses such as verifying cryptographic protocols. However, in cases where software exists with formal verification of its security properties, such software provides more assurance and trustworthiness and is preferred over similar software that has not been formally verified. The use of cryptographic signatures ensures the integrity and authenticity of critical and essential software that stores, processes, transmits, or protects CUI. Cryptographic signatures include digital signatures and the computation and application of signed hashes using asymmetric cryptography; protecting the confidentiality of the key used to generate the hash; and using the public key to verify the hash information.

FIPS 140-3 provides security requirements for cryptographic modules. FIPS 180-4 and FIPS

202 provide secure hash standards. FIPS 186-4 provides a digital signature standard. NIST SP 800-147 provides BIOS protection guidance. The NIST Roots of Trust project provides additional guidance.

CMMC Clarification: Systems that perform a critical security function or processing of highly valued CUI data may contain a Trusted Platform Module (TPM) version 1.2 or higher chip. The organization will configure the systems the organization has identified to use a secure boot process (i.e., verify the signature of the OS loader and all kernel objects match expected values) and key applications are authenticated before running them. These procedures ensure the integrity of the security critical software.

Example 1

You are the IT manager for your organization. You have been tasked with building a new server and the organization requires all servers to use a secure boot process. You follow the procedure published by the server vendor to go in to the BIOS settings and enable Secure Boot and install the operating system to use Secure Boot.

Example 2

You purchase desktop and laptop computers for your organization. Before placing an order for five new systems, you check with the vendor to confirm these systems all contain a TPM 2.0 chip. When the laptops are received, you follow the vendor's procedures to configure the systems to use Secure Boot, install the organization's standard security applications and test that everything is working correctly before making the laptops available for the new employees to use.

Mapping

- NIST SP 800-53R4: SI-7(6), SI-7(9), SI-7(10), SA-17
- NIST SP 800-171:
- CIS: 2.1
- CSF: PR.DS-6,PR.DS-8,PR.IP-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.1.076

Maturity Level 1

Capability C015: Grant access to authenticated entities

Practice IA.1.076: Identify information system users, processes acting on behalf of users, or devices.

Discussion: [DRAFT NIST SP 800-171 R2]: Common device identifiers include media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device. NIST SP 800-63-3 provides guidance on digital identities.

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

Example

You lead a project with the Department of Defense (DoD) for your small company and want to make sure that all employees working on the project can log on to the company system to see important information about the project. You also want to prevent employees who are not working on the DoD project from being able to access the information. You set up the system so that when an employee logs on, the system uniquely identifies each person, then determines the appropriate level of access.

Mapping

- NIST SP 800-53R4: IA-2, IA-3, IA-5
- NIST SP 800-171: 3.5.1
- CIS: 4.2,4.3,16.8,16.9
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Identify system users, processes acting on behalf of users, and devices.

NIST SP 800-171R2 Related Discussion: Common device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

Assessment

Assessment Objective(s): Determine if:

3.5.1[a] system users are identified.

3.5.1[b] processes acting on behalf of users are identified.

3.5.1[c] devices accessing the system are identified.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.1.077

Maturity Level 1

Capability C015: Grant access to authenticated entities

Practice IA.1.077: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

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

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

Some devices ship with default usernames and passwords. For example, some devices ship so that when you first logon to the device, the username is “admin” and the password is “admin”. When you have devices with this type of default username and password, you need to change the default password to a unique password you create. Default passwords are well known to the public, and easily found in a search. So, these default passwords would be easy for an unauthorized person to guess and use to gain access to your system.

Example

You are in charge of purchasing for your company. You know that some devices, such as laptops, come with a default username and a default password. Last week, your coworker in the Engineering Department received a laptop with the default username “admin” and default password “admin.” You remind the coworker to be sure to delete the default account details, or change the default password to a unique password. You also explain that default passwords are easily found in an internet search engine making it easy for an unauthorized person to gain access to the system.

Mapping

- NIST SP 800-53R4: IA-2, IA-3, IA-5
- NIST SP 800-171: 3.5.2

- CIS: 4.2,4.3,16.8,16.9
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

NIST SP 800-171R2 Related Discussion: Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

Assessment

Assessment Objective(s): Determine if:

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

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

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

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C015: Grant access to authenticated entities

Practice IA.2.078: Enforce a minimum password complexity and change of characters when new passwords are created.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

CMMC Clarification: Password complexity means using different types of characters as well as a specified number of characters. These include numbers, lowercase and uppercase letters, and symbols. Define the lowest level of password complexity required. Enforce this rule for all passwords.

Example

You are in charge of setting your organization's password rules. Everyone must use a combination of different types of characters for all new and changed passwords. Also, there is an established number of minimum characters for each password. Characters include numbers, lowercase and uppercase letters, and symbols. These rules help create hard-toguess passwords, which help to secure your network.

Mapping

- NIST SP 800-53R4: IA-5(1)
- NIST SP 800-171: 3.5.7
- CIS: 4.2,4.4
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Enforce a minimum password complexity and change of characters when new passwords are created.

NIST SP 800-171R2 Related Discussion: This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

Assessment

Assessment Objective(s): Determine if:

3.5.7[a] password complexity requirements are defined.

3.5.7[b] password change of character requirements are defined.

3.5.7[c] minimum password complexity requirements as defined are enforced when new passwords are created.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.2.079

Maturity Level 2

Capability C015: Grant access to authenticated entities

Practice IA.2.079: Prohibit password reuse for a specified number of generations.

Discussion: [DRAFT NIST SP 800-171 R2]: Password lifetime restrictions do not apply to temporary passwords.

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

Example

You are in charge of setting your organization's password rules. You define how often individuals can reuse their passwords and the minimum number of password generations before reuse. Using new passwords helps provide increased network security.

Mapping

- NIST SP 800-53R4: IA-5(1)
- NIST SP 800-171: 3.5.8
- CIS: 4.2,4.4
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Prohibit password reuse for a specified number of generations.

NIST SP 800-171R2 Related Discussion: Password lifetime restrictions do not apply to temporary passwords.

Assessment

Assessment Objective(s): Determine if:

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

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.2.080

Maturity Level 2

Capability C015: Grant access to authenticated entities

Practice IA.2.080: Allow temporary password use for system logons with an immediate change to a permanent password.

Discussion: [DRAFT NIST SP 800-171 R2]: Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

CMMC Clarification: Users must change their temporary passwords the first time they log in. Temporary passwords usually follow a consistent style within an organization and can be more easily guessed than passwords created by the unique user.

Example

You are in charge of setting temporary passwords for your users. Users must change their temporary passwords to a permanent password the first time they log in.

Mapping

- NIST SP 800-53R4: IA-5(1)
- NIST SP 800-171: 3.5.9
- CIS:
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Allow temporary password use for system logons with an immediate change to a permanent password.

NIST SP 800-171R2 Related Discussion: Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

Assessment

Assessment Objective(s): Determine if an immediate change to a permanent password is required when a temporary password is used for system logon.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.2.081

Maturity Level 2

Capability C015: Grant access to authenticated entities

Practice IA.2.081: Store and transmit only cryptographically-protected passwords.

Discussion: [DRAFT NIST SP 800-171 R2]: Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords.

See NIST Cryptographic Standards and Guidelines.

CMMC Clarification: All passwords must be cryptographically protected in a one-way function for storage and transmission. This type of protection changes passwords into another form, or a hashed password. A one-way transformation makes it impossible to turn the hashed password back into the original password.

Example

You are responsible for managing passwords for your organization. You protect all passwords with a one-way transformation, or hashing, before storing or transmitting them.

Mapping

- NIST SP 800-53R4: IA-5(1)
- NIST SP 800-171: 3.5.10
- CIS: 16.4,16.5
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Store and transmit only cryptographically-protected passwords.

NIST SP 800-171R2 Related Discussion: Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords. See [NIST CRYPTO].

Assessment

Assessment Objective(s): Determine if:

3.5.10[a] passwords are cryptographically protected in storage.

3.5.10[b] passwords are cryptographically protected in transit.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C015: Grant access to authenticated entities

Practice IA.2.082: Obscure feedback of authentication information.

Discussion: [DRAFT NIST SP 800-171 R2]: The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

CMMC Clarification: A password is a type of authentication information. When users enter this information, the system displays a symbol, such as an asterisk. This prevents others from seeing the actual characters. The organization should obscure feedback based on a defined policy. For example, smaller devices may briefly show characters before obscuring.

Example

You are in charge of IT for your company. You set up your systems to display a symbol, such as an asterisk, when users enter their passwords into a computer system. For your mobile devices, the password characters are briefly displayed to the user before being obscured. This prevents people from figuring out passwords by looking over someone's shoulder.

Mapping

- NIST SP 800-53R4: IA-6
- NIST SP 800-171: 3.5.11
- CIS:
- CSF: PR.AC-1

NIST SP 800-171R2 Related Security Requirement: Obscure feedback of authentication information.

NIST SP 800-171R2 Related Discussion: The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

Assessment

Assessment Objective(s): Determine if authentication information is obscured during the authentication process.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C015: Grant access to authenticated entities

Practice IA.3.083: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Discussion: [DRAFT NIST SP 800-171 R2]: Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challengeresponse authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security. Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.

CMMC Clarification: Implement a combination of two or more factors of authentication to verify privileged account holders' identity regardless of how the user is accessing the account. Implement a combination of two or more factors for non-privileged users requiring network access. These factors include:

- something you know (e.g., password/PIN);
- something you have (e.g., token); and
- something you are (e.g., biometrics).

Example

To improve security of your network you determine multifactor authentication (MFA) is necessary. Multifactor authentication will provide confirmation that the person attempting access is who they claim to be, and is not someone using a stolen password. As part of your plan for the IT infrastructure you enable multifactor authentication on your remote access point. When users initiate remote access they will be prompted for the additional authentication factor. Because your organization is also using a cloud-based application you enable MFA when staff access the application from within the office, at home, or on travel. Finally, you work to enable MFA for users who login into the network with their laptops and desktops. You configure your internal directory service to require MFA when a user authenticates to their system while on the network.

Mapping

- NIST SP 800-53R4: IA-2(1), IA-2(2), IA-2(3)
- NIST SP 800-171: 3.5.3
- CIS: 4.5,11.5,12.11
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

NIST SP 800-171R2 Related Discussion: Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security.

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

Assessment

Assessment Objective(s): Determine if:

3.5.3[a] privileged accounts are identified.

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

3.5.3[c] multifactor authentication is implemented for network access to privileged accounts.

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

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting or implementing multifactor authentication capability].

Testing Assessment Notes:

Maturity Level 3

Capability C015: Grant access to authenticated entities

Practice IA.3.084: Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Discussion: [DRAFT NIST SP 800-171 R2]: Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challengeresponse one-time authenticator.

CMMC Clarification: When insecure protocols are used for access to computing resources there is the potential for an adversary to perform a man-in-the-middle attack and capture the information that permitted a staff member to login. As part of a defense-in-depth strategy it is important to use mechanisms that are resilient to the adversary reusing the captured information and gaining access to the computing resources.

Example

To protect your IT organization, you understand that the methods for authentication must not be easily copied and re-sent to your systems by an adversary. You conduct research and determine certain protocols have replay resistance inherently designed into them. Your first step is to ensure Transport Layer Security (TLS) is enabled for access to relevant IT services. Coupled with the use of a secure protocol you evaluate the use of multifactor authentication using public key infrastructure (PKI) or one-time password tokens (OTP) to protect staff logins. Based on your requirements you select OTP tokens as the way to provide a timebound challenge for user authentication to your IT services.

Mapping

- NIST SP 800-53R4: IA-2(8), IA-2(9)
- NIST SP 800-171: 3.5.4
- CIS:
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.

NIST SP 800-171R2 Related Discussion: Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

Assessment

Assessment Objective(s): Determine if replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.3.085

Maturity Level 3

Capability C015: Grant access to authenticated entities

Practice IA.3.085: Prevent the reuse of identifiers for a defined period.

Discussion: [DRAFT NIST SP 800-171 R2]: Identifiers are provided for users, processes acting on behalf of users, or devices (IA.1.076). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

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

Example

As the IT administrator for your organization you maintain a central directory/domain that holds user accounts and computers within the organization. As part of your job you issue unique usernames (joe@acme.com) for the staff to access resources. When you issue staff computers you also rename the computer to reflect to whom it is assigned (joe-laptop01). Joe has recently left the organization so you must manage the former staff member's account. Incidentally, the replacement is also named Joe. In the directory you do not assign the previous account to the new user. You create an account called joe02. This account is assigned the appropriate permissions for the new user. A new laptop is also provided with the identifier of joe02-laptop01.

Mapping

- NIST SP 800-53R4: IA-4
- NIST SP 800-171: 3.5.5
- CIS: 16.7,16.10,16.12
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Prevent reuse of identifiers for a defined period.

NIST SP 800-171R2 Related Discussion: Identifiers are provided for users, processes acting on behalf of users, or devices (3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Assessment

Assessment Objective(s): Determine if:

3.5.5[a] a period within which identifiers cannot be reused is defined.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

IA: Identification and Authentication C015:IA.3.086

Maturity Level 3

Capability C015: Grant access to authenticated entities

Practice IA.3.086: Disable identifiers after a defined period of inactivity.

Discussion: [DRAFT NIST SP 800-171 R2]: Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.

CMMC Clarification: Identifiers are uniquely associated with an individual, group, role or device. An inactive identifier is one that has not been used for a certain period of time. For example, a user account may be needed for a certain time to allow for transition of business processes to existing or new staff. Once use of the identifier is no longer necessary it should be disabled and marked for deletion based on policy. Failure to maintain awareness of accounts that are no longer needed yet still active could be used by an adversary to exploit IT services. Example

You are the IT manager responsible for enforcing your company's inactive account policy: any account that has not been used in the last 45 days must be deleted. You decide to do this by writing a script that runs once a day to check the last login date for each account and generates a report of the accounts with no login records for the last 45 days. After reviewing the report, you notify the employee's supervisor and delete the account.

Mapping

- NIST SP 800-53R4: IA-4
- NIST SP 800-171: 3.5.6
- CIS: 16.9,16.10,16.11
- CSF: PR.AC-1,PR.AC-6,PR.AC-7

NIST SP 800-171R2 Related Security Requirement: Disable identifiers after a defined period of inactivity.

NIST SP 800-171R2 Related Discussion: Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.

Assessment

Assessment Objective(s): Determine if:

3.5.6[a] a period of inactivity after which an identifier is disabled is defined.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C016: Plan incident response

Practice IR.2.092: Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recover, and user response activities.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

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

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

CMMC Clarification: Incident handling should include activities that prepare your organization to respond to incidents. These activities may include the following:

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

You may need software and hardware to analyze incidents when they occur. You should also consider incident prevention activities as part of your incident-handling capability. The incident handling team provides input for such things as risk assessments and training.

Your organization should detect incidents in different ways. Use indicators to detect incidents. Indicators are things that don't look like what you expect. Examples include:

- alerts from your sensors or antivirus software;
- a filename that looks unusual; and
- a log entry that raises concern.

After you detect an incident, you should analyze it to decide what to do. To analyze an incident, you need to know what should be occurring on your network and what should not. This will help you determine when an incident may have occurred. It may also help you decide what to do about it. You should also document what you know about the incident. Include all the log entries associated with the incident in your documentation.

Containment of the incident is important. This stops the damage the incident is causing to your network. You should base the containment activities you do off your incident analysis. These activities can include:

- disconnecting a system from the internet; and
- changing firewall settings to stop an attack.

Recovery activities are things to fix that caused the incident. This will help prevent the incident happening again. Recovery activities also include things that fix the affected systems, including:

- restoring backup data; and
- reinstalling software.

User response activities include:

- performing a lessons-learned analysis;
- deciding if you should contact the police; and
- updating any policy or plans as a result of after incident analysis.

Example 1

Your manager asks you to set up your organization's incident-response capability. First, you create an email address to collect information on possible incidents. Next, you draft a contact list of all the people in the organization who need to know when an incident occurs. Then, you write down a procedure for how to submit incidents. This includes what everyone should do when a potential incident is detected or reported. The procedure also explains how to track incidents, from initial creation to closure.

Example 2

You receive an email alert about a possible incident. An employee identified a suspicious email message as a phishing attempt. First, you document the incident in your incident tracking system. Then, you immediately reference your defined procedures for handling incidents. For example, you send an email

to your employees alerting them not to open a similar email. You also start collecting information around the reported incident. Example 3

In response to the suspicious email, you perform a set of actions.

You reinstall the software on the machine of the user involved. This means that the individual no longer has an infected machine.

You update your phishing protection software. This ensures that it can block the latest phishing attacks.

You update your training material to emphasize the threat of phishing emails.

Mapping

- NIST SP 800-53R4: IR-2, IR-4
- NIST SP 800-171: 3.6.1
- CIS:
- CSF: RS.RP-1

NIST SP 800-171R2 Related Security Requirement: Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

NIST SP 800-171R2 Related Discussion: Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

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

Assessment

Assessment Objective(s): Determine if:

3.6.1[a] an operational incident-handling capability is established.

3.6.1[b] the operational incident-handling capability includes preparation.

3.6.1[c] the operational incident-handling capability includes detection.

3.6.1[d] the operational incident-handling capability includes analysis.

3.6.1[e] the operational incident-handling capability includes containment.

3.6.1[f] the operational incident-handling capability includes recovery.

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

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with incident response assistance and support resp

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 2

Capability C017: Detect and report events

Practice IR.2.093: Detect and report events.

Discussion: [CERT RMM V1.2]: The monitoring, identification, and reporting of events are the foundation for incident identification and commence the incident life cycle. Events potentially affect the productivity of organizational assets and, in turn, associated services. These events must be captured and analyzed so that the organization can determine whether an event will become (or has become) an incident that requires organizational action. The extent to which an organization can identify events improves its ability to manage and control incidents and their potential effects.

CMMC Clarification: Detect events on your network. An event is any observable occurrence on the network. You can detect events several ways, including through:

- observations of breakdowns in processes or loss in productivity;
- observations such as alarms and alerts, notification from other organizations; and
- the results of audits or assessments.

After you detect an event, determine if it will affect organizational assets and/or has the potential to disrupt operations. This may require the start of the incident process.

Example

You are in charge of IT operations for your company. As part of your role, you should track events on your network. You should also be a collection point for your coworkers to send you suspected events. When you discover or receive a report of an event, you should tell the person who will need to act on the detected event.

Mapping

- NIST SP 800-53R4: IR-6
- NIST SP 800-171:
- CIS: 19.4
- CSF: DE.CM-1,DE.CM-2,DE.CM-3,RS.CO-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C017: Detect and report events

Practice IR.2.094: Analyze and triage events to support event resolution and incident declaration.

Discussion: [CERT RMM V1.2]: The triage of event reports is an analysis activity that helps the organization to gather additional information for event resolution and to assist in incident declaration, handling, and response. Triage consists of categorizing, correlating, prioritizing, and analyzing events. Through triage, the organization determines the type and extent of an event (e.g., physical versus technical), whether the event correlates to other events (to determine if they are symptomatic of a larger issue, problem, or incident), and in what order events should be addressed or assigned for incident declaration, handling, and response. Triage also helps the organization to determine if the event needs to be escalated to other organizational or external staff (outside of the incident management staff) for additional analysis and resolution.

Some events will never proceed to incident declaration; the organization determines these events to be inconsequential. For events that the organization deems as low priority or of low impact or consequence, the triage process results in closure of the event and no further actions are performed.

Events that exit the triage process warranting additional attention may be referred to additional analysis processes for resolution or declared as an incident and subsequently referred to incident response processes for resolution. These events may be declared as incidents during triage, through further event analysis, through the application of incident declaration criteria, or during the development of response strategies, depending on the organization's incident criteria, the nature and timing of the event(s), and the consequences of the event that the organization is currently experiencing or that is imminent.

CMMC Clarification: Analyze events to determine what to do. Categorize, prioritize, or group events to determine how to handle the event. You can take different actions in response to an event:

- declare an incident from the event;
- escalate it to someone outside the organization; and
- close the event because it does not have a large consequence on the organization.

Example

You are in charge of IT operations for your company. As part of your role, you are the collection point for events. You should analyze all events to determine what actions to take. Through analysis, you should determine:

- the type and extent of an event (e.g., physical versus technical);
- whether the event is related to other events (to determine if they are part of a larger issue, problem, or incident); and
- in what order events should be addressed.

Analysis also helps the organization determine whether to escalate the event to external staff. If so, the external staff can perform analysis and resolution.

Mapping

- NIST SP 800-53R4: IR-4(3)
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C018: Develop and implement a response to declared incident

Practice IR.2.096: Develop and implement responses to declared incidents according to predefined procedures.

Discussion: [CERT RMM V1.2]: Responding to an organizational incident is often dependent on proper advance planning by the organization in establishing, defining, and staffing an incident management capability.

Responding to an incident describes the actions the organization takes to prevent or contain the impact of an incident on the organization while it is occurring or shortly after it has occurred. The range, scope, and breadth of the organizational response will vary widely depending on the nature of the incident. Incident response may be as simple as notifying users to avoid opening a specific type of email message or as complicated as having to implement service continuity plans that require relocation of services and operations to an off-site provider. The broad range of potential incidents requires the organization to have a broad range of capability in incident response.

CMMC Clarification: Write procedures ahead of time to use when responding to incidents. These procedures will help guide the development and implementation of responses during an incident. Responses should prevent or contain the impact of an incident while it is occurring or shortly after. The type of response will vary depending on the incident. Response actions might include:

- stopping or containing the damage (e.g., by taking hardware or systems offline);
- communicating to users (e.g., avoid opening a specific type of email message);
- communicating to stakeholders (e.g., corporate management); and
- implementing controls (e.g., updating access control lists).

Example

You are in charge of IT operations for your company. In this role, you manage all declared incidents. You have procedures in place for handling different types of declared incidents. For example, when you identify a phishing email incident, you have a process in place. You notify your company about the suspicious email and what to do when you receive it.

Mapping

- NIST SP 800-53R4: IR-4
- NIST SP 800-171:
- CIS: 19.1
- CSF: RS.RP-1

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C019: Perform post incident reviews

Practice IR.2.097: Perform root cause analysis on incidents to determine underlying causes.

Discussion: [CERT RMM V1.2]: Post-incident review is a formal part of the incident closure process. The organization conducts a formal examination of the causes of the incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the incident to occur.

Post-incident review should include a significant root-cause analysis process. The organization should employ commonly available techniques (such as cause-and-effect diagrams) to perform root-cause analysis as a means of potentially preventing future incidents of similar type and impact. Considerations of other processes that may have caused or aided the incident should be given, particularly as they may exist in processes such as change management and configuration management.

CMMC Clarification: Examine the causes of the event or incident and how your organization responded to it. Look at the administrative, technical, and physical control weaknesses. These may have allowed the incident to occur. Use available practices, such as cause-and-effect diagrams, to perform root-cause analysis. This will prevent future similar incidents. After incidents are resolved, conduct reviews and capture lessons learned. Make improvements based on the outcomes of these activities, such as updating plans or controls.

Example

You are in charge of IT operations for your company. As part of your role, you manage incident response. After incidents are resolved, you and your team conduct a root cause analysis. Doing this analysis helps you determine the underlying causes of declared incidents. Based on what you learn from the analysis, you can make changes to your network to prevent similar incidents.

Mapping

- NIST SP 800-53R4: AU-2
- NIST SP 800-171:
- CIS:
- CSF: DE.AE-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C018: Develop and implement a response to declared incident

Practice IR.3.098: Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Discussion: [DRAFT NIST SP 800-171 R2]: Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies.

CMMC Clarification: Incident response is a process an organization executes to manage the consequences and reduce the risk as a result of a security breach or cyberattack. The majority of the process consists of identification, containment, eradication, and recovery of the incident. During this process it is essential for an organization to track the work processes required in order to effectively respond. During the process the organization should designate a central hub to serve as the point to coordinate, communicate, and track activities. The hub should receive and document information from system administrators, incident handlers, and others involved throughout the process. As the incident process moves toward eradication the organization's executives, affected business units, and any required external stakeholders should be kept aware of the incident in order to make decisions affecting the business. Designated staff members should also be assigned to work with executives to provide communications outside the organization in event it is needed.

Example

As a database administrator you notice unusual activity on a server and determine a potential security incident has occurred. You open a tracking ticket with the Security Operations Center (SOC). The SOC assigns an incident handler to work the ticket. The incident handler investigates, collects artifacts, and documents initial findings. As a result of the investigation the incident handler determines unauthorized access occurred on the database server. The SOC establishes a team to manage the incident. The team consists of security, database, network, and system administrators. The team meets daily to update progress and plan courses of action to contain the incident. At the end of the day the team provides a status report to IT executives. Two days later the team declares the incident contained. The team produces a final report as the database system is rebuilt and placed back into operations.

Mapping

- NIST SP 800-53R4: IR-6, IR-7
- NIST SP 800-171: 3.6.2
- CIS: 19.4

- CSF: RS.CO-2,RS.CO-3

NIST SP 800-171R2 Related Security Requirement: Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

NIST SP 800-171R2 Related Discussion: Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies.

Assessment

Assessment Objective(s): Determine if:

3.6.2[a] incidents are tracked.

3.6.2[b] incidents are documented.

3.6.2[c] authorities to whom incidents are to be reported are identified.

3.6.2[d] organizational officials to whom incidents are to be reported are identified.

3.6.2[e] identified authorities are notified of incidents.

3.6.2[f] identified organizational officials are notified of incidents.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with incident monitoring responsibilities; personnel with incident reporting responsibilities; personnel who have or should have reported incidents; personnel (authorities) to whom incident information is to be reported; personnel

Interview Assessment Notes:

Test: [SELECT FROM: Incident monitoring capability for the organization; mechanisms supporting or implementing tracking and documenting of system security incidents; organizational processes for incident reporting; mechanisms supporting or implementing incident

Testing Assessment Notes:

Maturity Level 3

Capability C020: Test incident response

Practice IR.3.099: Test the organizational incident response capability.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

CMMC Clarification: Testing an organization's incident response capability validates existing plans as well as highlight lapses or changes within the environment. The test should seek to address questions like what happens during an incident, who is responsible for incident management, what tasks are assigned within the IT organization, what support would be needed from legal, public affairs, or other business component, how are resources obtained if needed during the incident, and how is law enforcement involved. Any negative impacts to the normal day-to-day mission when responding to an incident should also be identified and documented.

Example

As CISO, you decide to conduct an incident response table top exercise. The exercise plans to simulate an attacker gaining access to the network through a compromised server. When scheduling the exercise you include relevant IT staff such as security, database, network, and system administrators. You also request a representative from legal, HR, and the communications department. As the exercise begins you provide a scenario to the team. You have key questions aligned with the response plans to guide the exercise. During the exercise you focus on how the team executes the organization's incident response plan. At the end of the test, you conduct a debrief with everyone that was involved to provide feedback and develop improvements to the incident response plan.

Mapping

- NIST SP 800-53R4: IR-3
- NIST SP 800-171: 3.6.3
- CIS: 19.7
- CSF: DE.DP-3

NIST SP 800-171R2 Related Security Requirement: Test the organizational incident response capability.

NIST SP 800-171R2 Related Discussion: Organizations test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Assessment

Assessment Objective(s): Determine if the incident response capability is tested.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with incident response testing responsibilities; personnel with information security responsibilities; personnel with responsibilities for testing plans related to incident response].

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms and processes for incident response].

Testing Assessment Notes:

Maturity Level 4

Capability C016: Plan incident response

Practice IR.4.100: Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.

Discussion: [CMMC]: This practice requires that an organization explicitly consider the attacker's perspective in implementing the organization's incident response capability. The information necessary to do so can be from public sources, from government, or from third-party threat intelligence organizations. Specially, it is not the intent of this practice to require an internal, organizational threat intelligence capability. See practice RM.4.149 for the creation of this information.

CMMC Clarification: When conducting cyberattacks the attackers (or actors) tend to operate using certain patterns of behavior or exploit capabilities. These patterns and capabilities are known as Tactics, Techniques, and Procedures (TTPs). Knowledge of adversarial TTPs permits an organization to develop the right protective measures and responses to address a potential attack.

An organization can build their knowledge of attacker TTPs by participating in Information Sharing and Analysis Centers (ISAC) for their industry. An ISAC collects cyber threat information relevant to the industry and its members in order to improve the cyber posture of that industry. Based on the lines of business an organization may consider more than one ISAC.

Example

You are a manager. Your organization develops cutting edge technology for the aerospace and defense industry. Recent news indicates the industry is facing increased cyberattacks. Several peers share with you that they have experienced these attacks. To better understand the threats, you enroll the organization in the Aviation and National Defense ISACs. As part of the ISACs, you receive reports that help inform your organizational defenses. You attend ISAC meetings where peers share TTPs and best practices. Using what you learned, you conduct open source research on the Internet for additional information about attackers and how they conduct their operations. You use all of this information to improve incident response planning for the organization.

ADDITIONAL READING

National Council of ISACs: https://www.nationalisacs.org/

NSA/CSS Technical Cyber Threat Framework v2: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professionalresources/ctr-nsa-css-technical-cyber-threat-framework.pdf

ATT&CK: https://attack.mitre.org/

NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Mapping

- NIST SP 800-53R4:

- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C018: Develop and implement a response to declared incident

Practice IR.4.101: Establish and maintain a security operations center capability that facilitates a 24/7 response capability.

Discussion: [DRAFT NIST SP 800-171B (MODIFIED)]: A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers); and implements technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and securityrelevant event data from multiple sources. Sources include perimeter defenses, network devices (e.g., gateways, routers, switches) and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.

CMMC Clarification: As an organization matures it should dedicate resources to provide ongoing situational awareness. A security operations center (SOC) provides awareness through the ongoing collection of logs from the organization's various defensive capabilities on its network and endpoints. The SOC processes the logs and any associated alerts in order to quickly identify and remediate threats before more damage is caused. Thus, ongoing monitoring is key to an effective cyber posture. In addition to technology a SOC must be staffed by the appropriate personnel to ensure data is collected, analyzed, and investigated.

A SOC might be a physical facility, an organizational construct, or a managed service. Regardless of the SOC organization, it must enable a 24 hours a day, seven days a week response capability. An organization can determine how best to staff and create the response capability; 24/7 on-site staffing may not be required.

Example

You are the senior manager responsible for the organization's incident response. You have coordinated with a CMMC compliant third-party security services provider to include your organization in that provider's security operation center (SOC) coverage. The third-party SOC has established direct lines of communication between the SOC and your organization's incident response capability to effectively integrate the SOC into your organization's cybersecurity capabilities.

ADDITIONAL READING

NIST SP 800-61 provides guidance on incident handling. NIST SP 800-86 and SP 800-101 provide guidance on integrating forensic techniques into incident response. NIST SP 800150 provides guidance

on cyber threat information sharing. NIST SP 800-184 provides guidance on cybersecurity event recovery.

Ten Strategies of a World-class Cybersecurity Operations Center: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategiescyber-ops-center.pdf

SANS Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey: https://www.sans.org/media/analyst-program/common-practices-securityoperations-centers-results-2019-soc-survey-39060.pdf

DHS Cyber Resilience Review Supplemental Resource Guide Volume 5 Incident

Management: https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides /CRR_Resource_Guide-IM.pdf

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C016: Plan incident response

Practice IR.5.106: In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.

Discussion: [CMMC]: Organizations need to have the ability to gather attack forensics as part of responding to security incidents. During a cyberattack an attacker may seek to hide the activities taken to gain access, maintain persistence, and perform reconnaissance of an organization's networks. However, in the course of their activities the attackers will leave artifacts that indicate their presence. This could be a local event indicating a system login, files associated with malware, or processes running in the system memory. To avoid detection an attacker may erase local logs or delete files. To allow for a thorough investigation the security operations center (SOC) should seek to collect forensic data from systems in real-time and be able to collect volatile data such as system memory when needed. Collection of the forensic data should be protected during transit and storage.

CMMC Clarification: The security operations center (whether in-house or outsourced) must have the necessary forensic data to develop situational awareness across the organization's infrastructure. One solution identifies and collects security relevant system events, data, or images using an agent on the system. The agent transfers the events in real-time over a secure channel to a protected network enclave. Other solutions require physical access to the machine from which the data is gathered.

Many individual system security tools such as anti-virus or endpoint detection and response (EDR) tools can create logs, access system information in real-time, or image memory for secure transfer to a central management server. These logs would allow a SOC to begin the investigation. The SOC should also consider software tools used to push software or patches to systems. This would provide an on-demand capability for the SOC to send a security application when needed for forensic data collection.

Example

You are responsible for security operations at your organization. You implement a central log collection tool and configure your organization's laptops and desktops to send syslog and security event logs to this tool. The tool is used by the SOC staff to monitor for abnormal activity. When suspicious activity is detected, the SOC has access to an open source utility you have installed to collect additional forensic information from a target laptop or desktop about operating system process creation, network connections, and changes to files. This additional capability complements the security application forensic data.

ADDITIONAL READING

NIST Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final NIST Special Publication 800-86 Guide to Integrating Forensics Techniques into Incident

Response: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Mapping

- NIST SP 800-53R4: AU-12
- NIST SP 800-171:
- CIS:
- CSF: RS.AM-3

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C018: Develop and implement a response to declared incident

Practice IR.5.102: Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.

Discussion: [CMMC]: Response activities are necessary because the defenders of an organization's information technology tend to be at a disadvantage compared to the attacker. Defenders must maintain awareness of the latest vulnerabilities, be aware of the vulnerabilities in the organization, have the vulnerabilities remediated, and respond if an attacker finds a vulnerability before it is remediated. Once a vulnerability is discovered, the attacker tends to operates faster than a defender can match. To reduce the time to mitigate an organization should have plans in place to mitigate an attack. Plans must be comprehensive of manual and automated responses.

CMMC Clarification: To gain an advantage the organization should have pre-defined steps to reduce the risk from someone conducting a known pattern of malicious activity. The steps could be a manual checklist or automated series of actions using scripts or other technology. Organizations may call these pre-defined or automated lists a playbook or runbook. They help to establish a formalized incident response that can be performed. Organizations should balance the speed of response against the possibility of unintended side-effects in determining whether automated responses are appropriate.

Example

You are the security operations center (SOC) lead for your organization. Recently your organization has had a problem with staff inserting personal USB drives in their computers. The SOC has had to wait for the Helpdesk notification to respond. To reduce the response time to these incidents you build a workflow to respond to the use of personal USBs. First you identify the USB events from the host detection tool. The events are forwarded to the SOC event management application. Once identified, you create an alert that is triggered when the USB event is detected. You create a script to call the host detection management API to block further use of a personal USB.

ADDITIONAL READING

NIST Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Integrated Adaptive Cyber Defense: https://www.iacdautomate.org/

Mapping

- NIST SP 800-53R4: IR-4(1)
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C018: Develop and implement a response to declared incident

Practice IR.5.108: Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.

Discussion: [DRAFT NIST SP 800-171B]: A cyber incident response team (CIRT) is a team of experts that assesses, documents, and responds to cyber incidents so that organizational systems can recover quickly and implement the necessary controls to avoid future incidents. CIRT personnel typically include forensic analysts, malicious code analysts, systems security engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. The team members may or may not be full-time but need to be available to respond in the time period required. The size and specialties of the team are based on known and anticipated threats. The team is typically pre-equipped with the software and hardware (e.g., forensic tools) necessary for rapid identification, quarantine, mitigation, and recovery, and is familiar with how to preserve evidence and maintain chain of custody for law enforcement or counterintelligence uses. For some organizations the CIRT can be implemented as a cross organizational entity or as part of the Security Operations Center (SOC).

CMMC Clarification: An organization must have a team of individuals available to respond to a security incident within 24 hours. In the event of an incident the incident response team may need access to the network device or endpoint to investigate potential incidents. The response team may be able to perform the investigation virtually, or triage and quarantine virtually until local personnel can assist. The response team coordinates with information technology help desk personnel, system administrators, and physical security as appropriate to respond to an incident.

Example

You are the on-call cyber analyst for the organization's security operations center (SOC). During the night you receive a high priority notification. You quickly identify the source of the alert. A system in the London office indicates a potential compromise. You follow the SOC runbooks and execute the required incident response process. You send several commands to the system to collect running processes, dump the system memory, and identify new files. The data is collected back at the SOC in Chicago. Your initial analysis indicates the system should be isolated to mitigate any risk so you run the script that isolates the system on the network. The system is placed into a remediation VLAN for additional investigation. You send an update to the system administrators in London and mark the incident for follow-up by the morning shift SOC analysts in Chicago. At the start of your next shift, you see in the notes that the SOC analysts worked with the system administrators in London to resolve the incident.

ADDITIONAL READING

Ten Strategies of a World-class Cybersecurity Operations Center:
https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategiescyber-ops-center.pdf

SANS Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey: https://www.sans.org/media/analyst-program/common-practices-securityoperations-centers-results-2019-soc-survey-39060.pdf

DHS Cyber Resilience Review Supplemental Resource Guide Volume 5 Incident Management: https://www.uscert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C020: Test incident response

Practice IR.5.110: Perform unannounced operational exercises to demonstrate technical and procedural responses.

Discussion: [CMMC]: An organization is stronger against a cyber-attack when the incident response capability is proven to be able to handle a live incident. Operational exercises require the use of the operational environment by the staffed, operational personnel; they are not performed in a test environment. By performing this practice an organization is testing their incident response capabilities and procedures as outlined in the IR plan. These tests should be built specifically to launch the organization's IR process. This will involve the cyber defenders walking through the procedures as well as using their technical solutions. Preparation for an operational exercise might include performing a tabletop exercise to walk through the process. This will help identify shortfalls in the process.

CMMC Clarification: This practice requires a company to be able to plan and initiate an incident response exercise without the incident response team knowing it is going to happen. This is not about planning an IR test with all parties involved. The purpose of this practice is to test the IR team and the solutions, without a priori knowledge so the incident will help identify gaps in the current procedure or technical solutions. All findings should be used within a feedback loop to improve the IR procedures and to identify any technical shortfalls. This feedback will help the organization prioritize the changes towards future modification.

Example 1

You are the CISO of the organization. You have been asked by the CIO to run a no notice event to test the incident response of the cyber defense and/or response team. You are not allowed to tell the team prior to the event starting. This request was made by the CIO for a realistic event. You bring in a couple of your internal red team members and work with them to plan a few local incidents to exercise the IR capabilities as created. After developing the plan, you authorize the red team to launch the tests at 7AM on a Monday morning. You have an employee sit (white cell) in with the DCO team and another with the red team right before the incident response tests are launched. Each member of the white cell is asked to take detailed notes on what is perceived at each location. This information is compiled and presented to the CISO and the CIO at some future point. The information helps identify areas of concern and build a prioritization for future modifications to the process.

Example 2

You are the CISO of the organization. You have your red team borrow an admin account for a server in the data center, after the admins create an account for you. You have already worked with the red team and created a couple incidents that will help test the IR capability in a remote datacenter. This will help identify if the right tools and procedures are in place to handle a remote incident. You authorize the red team to launch the tests on a Friday evening when people are not typically at their desk. You have an employee sit (white cell) in with the DCO team (in this case, monitor their chat line) and another with the red team right before the incident response tests are launched. Each member of the white cell is asked to take detailed notes on what is perceived at each location. This information is compiled and

presented to the CISO and the CIO at some future point. The information helps identify areas of concern and build a prioritization for future modifications to the process.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 19.7
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C021: Manage maintenance

Practice MA.2.111: Perform maintenance on organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

CMMC Clarification: Perform maintenance on your machines. This includes:

- corrective maintenance (e.g., repairing problems with the technology);
- preventative maintenance (e.g., updates to prevent potential problems);
- adaptive maintenance (e.g., changes to the operative environment); and
- perfective maintenance (e.g., improve operations).

Example

You are in charge of IT at your company. As part of your role, you must perform maintenance on all the machines within your company. This includes regular planned maintenance, unscheduled maintenance, reconfigurations when required, and damage repairs. In addition to performing maintenance, you also keep track of all maintenance performed.

Mapping

- NIST SP 800-53R4: MA-2
- NIST SP 800-171: 3.7.1
- CIS:
- CSF: PR.MA-1

NIST SP 800-171R2 Related Security Requirement: Perform maintenance on organizational systems.

NIST SP 800-171R2 Related Discussion: This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

Assessment

Assessment Objective(s): Determine if system maintenance is performed.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing cont

Testing Assessment Notes:

Maturity Level 2

Capability C021: Manage maintenance

Practice MA.2.112: Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

CMMC Clarification: Protect the tools used to perform maintenance. They must remain secure so they don't introduce software viruses or other bugs into your system. Protect your maintenance processes so they aren't used to hurt your network. Supervise the people responsible for maintenance activities. Make sure they don't behave in a malicious manner.

Example

You are responsible for maintenance activities on your company's machines. These activities can introduce software viruses or bugs into your system. To prevent this, make sure your maintenance tools protect from unauthorized access. Also, confirm that your organization manages or supervises everyone assigned to perform maintenance.

Mapping

- NIST SP 800-53R4: MA-3
- NIST SP 800-171: 3.7.2
- CIS:
- CSF: PR.MA-1

NIST SP 800-171R2 Related Security Requirement: Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

NIST SP 800-171R2 Related Discussion: This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the

controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

Assessment

Assessment Objective(s): Determine if:

3.7.2[a] tools used to conduct system maintenance are controlled.

3.7.2[b] techniques used to conduct system maintenance are controlled.

3.7.2[c] mechanisms used to conduct system maintenance are controlled.

3.7.2[d] personnel used to conduct system maintenance are controlled.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; m

Testing Assessment Notes:

Maturity Level 2

Capability C021: Manage maintenance

Practice MA.2.113: Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Discussion: [DRAFT NIST SP 800-171 R2]: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA.3.083.

CMMC Clarification: Nonlocal maintenance activities must use multifactor authentication. Multifactor authentication requires at least two things to prove who the user says he is. One thing can be something you have, such as a device that generates a one-time passcode. Another thing can be something you know, for example, a password or passphrase. Or, another thing can be something specific to you, such as a fingerprint. Requiring two or more things to prove your identity increases the security of the connection. Nonlocal maintenance activities are activities conducted from external network connections. After nonlocal maintenance activities are complete, shut down the external network connection.

Example

You are in charge of conducting maintenance for your organization. You are an employee working remotely. You establish a remote connection to the company's network using the company's VPN solution. When you log on to the remote connection, you must provide a one-time passcode and a token generated by a token device. You need both of these things to prove your identity. After you enter your password and passcode, you have access to the maintenance remote connection. When you finish your activities, you shut down the remote connection.

Mapping

- NIST SP 800-53R4: MA-4
- NIST SP 800-171: 3.7.5
- CIS:
- CSF: PR.MA-2

NIST SP 800-171R2 Related Security Requirement: Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

NIST SP 800-171R2 Related Discussion: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

Assessment

Assessment Objective(s): Determine if:

3.7.5[a] multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.

3.7.5[b] nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System maintenance policy; procedures addressing nonlocal system maintenance; system security plan; system design documentation; system configuration

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel].

Testing Assessment Notes:

Maturity Level 2

Capability C021: Manage maintenance

Practice MA.2.114: Supervise the maintenance activities of personnel without required access authorization.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while PE.1.131 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

CMMC Clarification: You must supervise everyone who performs maintenance activities. Sometimes a person without proper permissions has to perform maintenance on your machines. Give that individual a logon that is active only once or for a very limited time, to limit system access.

Example

You are in charge of IT operations for your company. One of your software providers has to come on-site to update the software on your company's machines. You give the individual a temporary logon and password that expires in 12 hours. This gives him access long enough to perform the update. When he is on site, you remain with him. You supervise his activities. This ensures that he performs only the maintenance activities you directed.

Mapping

- NIST SP 800-53R4: MA-5
- NIST SP 800-171: 3.7.6
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Supervise the maintenance activities of maintenance personnel without required access authorization.

NIST SP 800-171R2 Related Discussion: This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations

may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

Assessment

Assessment Objective(s): Determine if maintenance personnel without required access authorization are supervised during maintenance activities.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel].

Testing Assessment Notes:

Maturity Level 3

Capability C021: Manage maintenance

Practice MA.3.115: Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

CMMC Clarification: Sanitization is a process that makes access to data infeasible on media such as a hard drive. The process may overwrite the entire media with a fixed pattern such as binary zeros. In addition to clearing the data an organization could purge (e.g., degaussing, secure erasing, or disassembling) the data, or even destroy the media (e.g., incinerating, shredding, or pulverizing). By performing one of these activities the data is extremely hard to recover, thus ensuring its confidentiality.

If additional guidance on which specific santization actions should be taken on any specific type of media, consider reviewing the description of the Purge actions given in NIST SP 80088 Revision 1 - Guidelines for Media Sanitization.

Example

You manage the IT equipment that is used for your organization. A recent Department of Defense (DoD) project has been using a storage array for DoD Controlled Unclassified Information (CUI). Recently the array has experienced disk issues. After troubleshooting with the vendor they recommend several drives be replaced in the array. Knowing the drives may have CUI information you plan to run software on the drives using software that performs a wipe pattern that removes any data and device protection across the entire drive. Once all the drives have been wiped you document the action and ship the faulty drives to the vendor.

Mapping

- NIST SP 800-53R4: MA-2
- NIST SP 800-171: 3.7.3
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Ensure equipment removed for off-site maintenance is sanitized of any CUI.

NIST SP 800-171R2 Related Discussion: This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement).

Assessment

Assessment Objective(s): Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing cont

Testing Assessment Notes:

Maturity Level 3

Capability C021: Manage maintenance

Practice MA.3.116: Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

CMMC Clarification: As part of troubleshooting a vendor may provide a diagnostic application to install on a system. The vendor is using the application to help identify the cause of issues on the system. As this is executable code there is a chance that the file is corrupt or infected with malicious code. Implement procedures to scan any files prior to installation. The same level of scrutiny must be made as with any file a staff member may download.

Example

You've recently been experiencing performance issues on one of your servers. After troubleshooting for much of the morning the vendor has asked to install a utility that will collect more data from the server. The file is stored on their FTP server. The support technician gives you the FTP site so you can anonymously download the utility file. You also ask him for a hash of the utility file. As you download the file to your local computer you realize it is compressed. While you have anti-virus on your server you don't want to cause any issues that may further impact business operations. On your desktop you unzip the file. Once the file is unzipped you open your local anti-virus and perform a manual scan of the utility file. The scan reports no issues. To further verify the utility file has not been tampered you run an application to see that the hash from the vendor matches.

Mapping

- NIST SP 800-53R4: MA-3(2)
- NIST SP 800-171: 3.7.4
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

NIST SP 800-171R2 Related Discussion: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

Assessment

Assessment Objective(s): Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

Testing Assessment Notes:

Maturity Level 1

Capability C024: Sanitize media

Practice MP.1.118: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization.

Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information. NIST SP 800-88 provides guidance on media sanitization.

CMMC Clarification: In this case, “media” can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones. It is important to see what information is on these types of media. If there is Federal contract information (FCI)—information you or your company got doing work for the Federal government that is not shared publicly)—you or someone in your company should do one of two things before throwing the media away:

- clean or purge the information, if you want to reuse the device; or
- shred or destroy the device so it cannot be read.

See NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization for more information.

Example

You are moving into a new office. As you pack for the move, you find some of your old CDs in a file cabinet. When you load the CDs into your computer drive, you see that one has information about an old project your company did for the Department of Defense (DoD).

Rather than throw the CD in the trash, you make sure that it is shredded.

Mapping

- NIST SP 800-53R4: MP-6
- NIST SP 800-171: 3.8.3
- CIS:
- CSF: PR.DS-3

NIST SP 800-171R2 Related Security Requirement: Sanitize or destroy system media containing CUI before disposal or release for reuse.

NIST SP 800-171R2 Related Discussion: This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

Assessment

Assessment Objective(s): Determine if:

3.8.3[a] system media containing CUI is sanitized or destroyed before disposal.

3.8.3[b] system media containing CUI is sanitized before it is released for reuse.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with media sanitization responsibilities; personnel with information security responsibilities; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for media sanitization; mechanisms supporting or implementing media sanitization].

Testing Assessment Notes:

Maturity Level 2

Capability C023: Protect and control media

Practice MP.2.119: Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Discussion: [DRAFT NIST SP 800-171 R2]: System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

NIST SP 800-111 provides guidance on storage encryption technologies for end user devices. CMMC CLARIFICATION

Physical CUI includes two types of items:

- hardcopy (e.g., paper, microfilm); and
- digital devices (e.g., CD drives, flash drives, video).

You should store physical CUI in a secure location. This location should be accessible only to those people with the proper permissions. All who access CUI should follow the process for checking out and returning it.

Example

Your organization has CUI for a specific Army contract. The Army gave you the CUI on a CD. You store the CD in a locked drawer and you log the CUI CD in an inventory. You also establish a procedure to check out the CD when your employees need to use it.

CMMC Clarification:

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171: 3.8.1
- CIS:
- CSF: PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

NIST SP 800-171R2 Related Discussion: System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

Assessment

Assessment Objective(s): Determine if:

3.8.1[a] paper media containing CUI is physically controlled.

3.8.1[b] digital media containing CUI is physically controlled.

3.8.1[c] paper media containing CUI is securely stored.

3.8.1[d] digital media containing CUI is securely stored.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].

Testing Assessment Notes:

Maturity Level 2

Capability C023: Protect and control media

Practice MP.2.120: Limit access to CUI on system media to authorized users.

Discussion: [DRAFT NIST SP 800-171 R2]: Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

CMMC Clarification: Limit physical access to CUI to people permitted to access CUI. Use locked or controlled storage areas and limit access to only those allowed to access CUI. Keep track of who accesses physical CUI in some sort of record.

Example

Your organization has CUI for a specific Army contract. The Army gave you the CUI on a CD. You store the CD in a locked drawer. The only employees with access to the drawer are those assigned to the project. They are the only people allowed to access CUI. When someone removes the CD for work, they sign it out with their name and time. When they return the CD to the locked drawer, they sign it back in.

Mapping

- NIST SP 800-53R4: MP-2
- NIST SP 800-171: 3.8.2
- CIS: 14.6
- CSF: PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Limit access to CUI on system media to authorized users.

NIST SP 800-171R2 Related Discussion: Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Assessment

Assessment Objective(s): Determine if access to CUI on system media is limited to authorized users.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

Testing Assessment Notes:

Maturity Level 2

Capability C023: Protect and control media

Practice MP.2.121: Control the use of removable media on system components.

Discussion: [DRAFT NIST SP 800-171 R2]: In contrast to requirement MP.2.119, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices. Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. Many technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

CMMC Clarification: Removable media is any type of media storage that you can remove from your computer or machine, for example, CDs, DVDs, diskettes and USB drives. Write a specific policy for removable media for your company. The policy should cover that there are two types of removable media: write-once media and rewritable media. Limit the use of removable media to the smallest number needed. Scan all removable media for viruses. Track removable media that you own and make sure you reuse and dispose of it properly. Example

You are in charge of IT operations at your company. You establish a policy for USB drives. All of them must be scanned for viruses and bugs before use on the company's networks. You set up a separate computer to scan these drives before anyone uses them on the network. This computer has anti-virus software installed that is kept up to date.

Mapping

- NIST SP 800-53R4: MP-7
- NIST SP 800-171: 3.8.7
- CIS: 13.7,13.8

- CSF: PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Control the use of removable media on system components.

NIST SP 800-171R2 Related Discussion: In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable

Assessment

Assessment Objective(s): Determine if the use of removable media on system components is controlled.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for media use; mechanisms restricting or prohibiting use of system media on systems or system components].

Testing Assessment Notes:

Maturity Level 3

Capability C022: Identify and mark media

Practice MP.3.122: Mark media with necessary CUI markings and distribution limitations.

Discussion: [DRAFT NIST SP 800-171 R2]: The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations.

CMMC Clarification: All media (e.g., USB drives, CDs, DVDs, diskettes, hard drives, and paper) must be properly marked to alert individuals to the presence of Controlled Unclassified Information (CUI) stored on the media. Since the media itself may be small and provide limited space to mark it you should at a minimum mark it as "Controlled" or CUI" and the designating agency. If the media is hard to mark alternate methods may be approved to indicate the presence of CUI. For example, a company may place a CUI banner on the desktop background image or monitor attached to the system. They could also require the user to accept a banner message stating CUI may be present on the system.

Example

You were recently contacted by the project manager for a new Department of Defense program at your company. The project manager said she wanted the CUI with the program properly protected. After speaking with her, most of the protections will be provided as part of the organization's cybersecurity capabilities infrastructure. She also mentions that the project team will use several USB drives to share certain data sets. You tell her that the USB drives the organization provides have encryption built into the device. You explain while this protects the confidentiality of the data the team must ensure the USB drives are externally marked to indicate the presence of CUI. The project manager thanks you for the reminder and has her team label the outside of each USB drive with an appropriate CUI label.

Mapping

- NIST SP 800-53R4: MP-3
- NIST SP 800-171: 3.8.4
- CIS:
- CSF: PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Mark media with necessary CUI markings and distribution limitations.

NIST SP 800-171R2 Related Discussion: The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. See [NARA MARK].

Assessment

Assessment Objective(s): Determine if:

3.8.4[a] media containing CUI is marked with applicable CUI markings.

3.8.4[b] media containing CUI is marked with distribution limitations.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; procedures addressing media marking; physical and environmental protection policy and procedures; system security plan; list of system media marking security attributes; designated controlled areas; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media protection and marking responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for marking information media; mechanisms supporting or implementing media marking].

Testing Assessment Notes:

Maturity Level 3

Capability C023: Protect and control media

Practice MP.3.123: Prohibit the use of portable storage devices when such devices have no identifiable owner.

Discussion: [DRAFT NIST SP 800-171 R2]: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

CMMC Clarification: A portable storage device is a small hard drive or solid state device that is designed to hold various types of data. It typically plugs into a laptop or desktop port (e.g., USB port). Due to the small size of the device they can be easily lost. This makes the portable storage device an attractive tool to hack an organization. Since the device can hold any type of file it could contain an executable or document that a staff member opens to determine who owns the portable storage device Therefore, an organization should prohibit use if it cannot trace the device to an owner.

Example

You are the IT manager for your organization. As you enter the building a staff member says they found a USB drive in the parking lot. You ask if the USB device indicates who might be the owner. The staff member responds that there didn't appear to be any special markings on the drive. Once they get to their office they plan to plug the drive into their laptop to see what type of files are on the drive. The data might indicate which project owns it. You remind them that IT policies and practices expressly prohibit plugging unknown devices into computers. You remind the staff member that your organization's IT policy directs them to turn in the lost USB device to the IT Helpdesk so they can resolve the issue.

Mapping

- NIST SP 800-53R4: MP-7(1)
- NIST SP 800-171: 3.8.8
- CIS:
- CSF: PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Prohibit the use of portable storage devices when such devices have no identifiable owner.

NIST SP 800-171R2 Related Discussion: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

Assessment

Assessment Objective(s): Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system configuration settings and associated documentation; system design documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for media use; mechanisms prohibiting use of media on systems or system components].

Testing Assessment Notes:

Maturity Level 3

Capability C025: Protect media during transport

Practice MP.3.124: Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Discussion: [DRAFT NIST SP 800-171 R2]: Controlled areas are areas or spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information. Controls to maintain accountability for media during transport include locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

CMMC Clarification: Protection of Controlled Unclassified Information (CUI) is applicable to physical and digital formats. Physical control can be accomplished using traditional concepts like restricted access to physical locations or locking papers in a desk or filing cabinet. The digitization of data makes access to CUI much easier. CUI can be stored and transported on magnetic disks, tapes, USB drives, CD-ROMs, and so on. This makes digital CUI data very portable. As a result of the portability it is important for an organization to apply mechanisms to prevent unauthorized access to CUI.

Example 1

Your organization recently was awarded a Department of Defense (DoD) contract. The contract requires processing of Controlled Unclassified Information (CUI). While reviewing the security requirements you read about controlling access to media. Aspects of your project will require machining specific parts for a DoD platform. The parts will be made in a room where the CUI is stored. The machining tool references the CUI data to produce the part. The room is isolated but generally accessible to all staff. To ensure you meet the requirements to protect the data you decide to install a separate badge reader on the door to the room. The badge reader will be used to restrict and log access to staff on the project. . You also write a policy requiring all portable media or printed documents containing CUI to be stored in the locked filing cabinets installed in the room and to require each person entering the room to badge in with no access allowed for those who have not been issued a badge. You train all employees on this policy when you issue them their new badge.

Example 2

Your team has recently completed setup of a server. The sponsor has asked that it be ready to plug in and use. You are aware that the application code created for the sponsor is considered to be Controlled Unclassified Information (CUI). As you box the server for shipment using tamper-evident packaging, you label it with the specific recipient for the shipment. You will also be using a shipping service so you will

get a tracking number to monitor the progress. Once completed you send the recipient the tracking number so they can monitor and ensure prompt delivery at their facility.

Mapping

- NIST SP 800-53R4: MP-5
- NIST SP 800-171: 3.8.5
- CIS:
- CSF: PR.PT-2

NIST SP 800-171R2 Related Security Requirement: Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

NIST SP 800-171R2 Related Discussion: Controlled areas are areas or spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information. Controls to maintain accountability for media during transport include locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

Assessment

Assessment Objective(s): Determine if:

3.8.5[a] access to media containing CUI is controlled.

3.8.5[b] accountability for media containing CUI is maintained during transport outside of controlled areas.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities; system or network administrators].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing media storage and media protection].

Testing Assessment Notes:

Maturity Level 3

Capability C025: Protect media during transport

Practice MP.3.125: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives).

CMMC Clarification: CUI can be stored and transported on a variety of media like magnetic disks, tapes, USB drives, CD-ROMs, and so on. This makes digital CUI data very portable. The portability increases the chance that the media is lost. When identifying the paths CUI flows through your organization, identify devices to include in this practice.

To mitigate the risk of losing or exposing CUI an organization should implement an encryption scheme to protect the data. Even if the media is lost the fact that it is properly encrypted renders the data inaccessible to other people. When encryption is not an option, alternative physical sageguards should be applied during transport.

Example

You manage the backups for file servers in your datacenter. In addition to the organization‘s sensitive information you know that CUI is stored on the file servers. As part of a broader plan to protect data your organization has begun sending the backup tapes off-site to a vendor. You are aware that your backup software provides the option to encrypt data onto tape. You develop a plan to test and enable backup encryption for the data sent off site. This will encrypt the data on the backup tapes while they are being transported.

Mapping

- NIST SP 800-53R4: MP-5(4)
- NIST SP 800-171: 3.8.6
- CIS: 13.9
- CSF:

NIST SP 800-171R2 Related Security Requirement: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

NIST SP 800-171R2 Related Discussion: This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). See [NIST CRYPTO].

Assessment

Assessment Objective(s): Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings and associated documentation; system media transport records; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system media transport responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas].

Testing Assessment Notes:

Maturity Level 2

Capability C026: Screen personnel

Practice PS.2.127: Screen individuals prior to authorizing access to organizational systems containing CUI.

Discussion: [DRAFT NIST SP 800-171 R2]: Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

CMMC Clarification: Make sure all employees who need access to CUI have the organization-defined screening before they get access. Base the types of screening on the requirements defined for that specific level of access.

Example

You are in charge of security at your organization. All individuals you hire must have proper screening before they can access CUI. Screening may include activities such as background checks and drug testing. Follow the appropriate laws, policies, regulations, and criteria for the level of access required for each position.

Mapping

- NIST SP 800-53R4: PS-3
- NIST SP 800-171: 3.9.1
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Screen individuals prior to authorizing access to organizational systems containing CUI.

NIST SP 800-171R2 Related Discussion: Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

Assessment

Assessment Objective(s): Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with personnel security responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for personnel screening].

Testing Assessment Notes:

Maturity Level 2

Capability C027: Protect CUI during personnel operations

Practice PS.2.128: Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Discussion: [DRAFT NIST SP 800-171 R2]: Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

CMMC Clarification: Make sure employees no longer have access to CUI when they change jobs or leave the company. Confirm that when an employee leaves:

- all company IT equipment (e.g., laptops, cell phones, storage devices) is returned;
- all of their identification/access cards and/or keys are returned; and
- an exit interview is conducted to remind the employee of their obligations to not discuss CUI, even after employment.

The organization will do the following:

- erase all equipment before reuse;
- remove access to all accounts granting access to CUI;
- disable or close employee accounts; and
- limit access to physical spaces with CUI.

Example

You are in charge of IT operations at your company. When someone leaves the company, you remove them from any physical CUI access lists. You contact them immediately, and ask them to:

- turn in their computers for proper handling which includes IT disabling all accounts; • return all their identification and access cards; and
- attend an exit interview where you remind them of their obligations to not discuss CUI.

Mapping

- NIST SP 800-53R4: PS-4, PS-5
- NIST SP 800-171: 3.9.2
- CIS:
- CSF: PR.AC-1

NIST SP 800-171R2 Related Security Requirement: Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

NIST SP 800-171R2 Related Discussion: Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Assessment

Assessment Objective(s): Determine if:

3.9.2[a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.

3.9.2[b] system access and credentials are terminated consistent with personnel actions such as termination or transfer.

3.9.2[c] the system is protected during and after personnel transfer actions.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked authenticators and credentials; records of exit interviews; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for personnel transfer and termination; mechanisms supporting or implementing personnel transfer and termination notifications; mechanisms for disabling system access and revoking authenticators].

Testing Assessment Notes:

Maturity Level 1

Capability C028: Limit physical access

Practice PE.1.131: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

CMMC Clarification: Think about what parts of your physical space (e.g., office, plant, factory), what equipment, including the network, need to be protected from physical contact. For those parts of your company to which you want only specific employees to have physical access, monitor or limit who is able to enter those spaces with badges, key cards, etc.

Example

You work for a small company as the project manager for a Department of Defense (DoD) project. The project requires special equipment that should be used only by project team members. You work with your boss to put locks on the doors to your area. This restricts access to the room to only those employees who work on the DoD project.

Mapping

- NIST SP 800-53R4: PE-2
- NIST SP 800-171: 3.10.1
- CIS:
- CSF: PR.AC-2

NIST SP 800-171R2 Related Security Requirement: Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

NIST SP 800-171R2 Related Discussion: This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

Assessment

Assessment Objective(s): Determine if:

3.10.1[a] authorized individuals allowed physical access are identified.

3.10.1[b] physical access to organizational systems is limited to authorized individuals.

3.10.1[c] physical access to equipment is limited to authorized individuals.

3.10.1[d] physical access to operating environments is limited to authorized individuals.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations].

Testing Assessment Notes:

Maturity Level 1

Capability C028: Limit physical access

Practice PE.1.132: Escort visitors and monitor visitor activity.

Discussion: [DRAFT NIST SP 800-171 R2]: Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

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

Example

Coming back from a meeting, you see the friend of a coworker walking down the hallway near your office. You know this person well and trust them, but are not sure why they are in the building. You stop to talk, and the person explains that they are supposed to meet the coworker for lunch, but cannot remember where the lunchroom is. You offer to walk the person back to the reception area to get a visitor badge and wait until someone can escort them to the lunch room. You report this incident, and the company decides to install a badge reader at the main door so visitors cannot enter without an escort.

Mapping

- NIST SP 800-53R4: PE-3
- NIST SP 800-171: 3.10.3
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Escort visitors and monitor visitor activity.

NIST SP 800-171R2 Related Discussion: Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

Assessment

Assessment Objective(s): Determine if:

3.10.3[a] visitors are escorted.

3.10.3[b] visitor activity is monitored.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel]

Testing Assessment Notes:

Maturity Level 1

Capability C028: Limit physical access

Practice PE.1.133: Maintain audit logs of physical access.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

CMMC Clarification: Make sure you have a record of who is accessing both your facility (e.g., office, plant, factory) and your equipment. You can do this in writing by having employees and visitors sign in and sign out as they enter and leave your physical space, and by keeping a record of who is coming and going from the facility.

Example

You and your coworkers like to have friends and family join you for lunch at the office on Fridays. Your small company is growing, and sometimes it's hard to know who is coming and going from the lunch area. You work with your boss, the company founder, and ask all non-employees to sign in at the reception area, then sign out when they leave. Employees can have badges or key cards that enable tracking and logging access to the company facilities.

Mapping

- NIST SP 800-53R4: PE-3
- NIST SP 800-171: 3.10.4
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Maintain audit logs of physical access.

NIST SP 800-171R2 Related Discussion: Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

Assessment

Assessment Objective(s): Determine if audit logs of physical access are maintained.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel]

Testing Assessment Notes:

Maturity Level 1

Capability C028: Limit physical access

Practice PE.1.134: Control and manage physical access devices.

Discussion: [DRAFT NIST SP 800-171 R2]: Physical access devices include keys, locks, combinations, and card readers.

CMMC Clarification: Controlling physical access devices like locks, badging, key cards, etc. is just as important as monitoring and limiting who is able to physically access certain equipment. Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.

Example

A team member retired last week and forgot to turn in company items, including an identification badge and office keys. The project requires special equipment that should be used only by project team members. Before you begin looking for a replacement employee, you make sure to change the locks on the doors to the project area. You also disable the retired team member's badge.

Mapping

- NIST SP 800-53R4: PE-3
- NIST SP 800-171: 3.10.5
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Control and manage physical access devices.

NIST SP 800-171R2 Related Discussion: Physical access devices include keys, locks, combinations, and card readers.

Assessment

Assessment Objective(s): Determine if:

3.10.5[a] physical access devices are identified.

3.10.5[b] physical access devices are controlled.

3.10.5[c] physical access devices are managed.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records;

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel]

Testing Assessment Notes:

PE: Physical Protection C028:PE.2.135

Maturity Level 2

Capability C028: Limit physical access

Practice PE.2.135: Protect and monitor the physical facility and support infrastructure for organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

CMMC Clarification: Make sure that the infrastructure inside of your facility, such as power and network cables, is protected so that visitors and employees cannot access it. The protection also has to be monitored. This can be done with security guards, video cameras, sensors and alarms.

Example

You are responsible for protecting your organization's IT facilities. You install video monitoring at each entrance and exit. You also make sure there are secure locks on all entrances and exits to the facilities.

Mapping

- NIST SP 800-53R4: PE-6
- NIST SP 800-171: 3.10.2
- CIS:
- CSF: PR.AC-2

NIST SP 800-171R2 Related Security Requirement: Protect and monitor the physical facility and support infrastructure for organizational systems.

NIST SP 800-171R2 Related Discussion: Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

Assessment

Assessment Objective(s): Determine if:

3.10.2[a] the physical facility where organizational systems reside is protected.

3.10.2[b] the support infrastructure for organizational systems is protected.

3.10.2[c] the physical facility where organizational systems reside is monitored.

3.10.2[d] the support infrastructure for organizational systems is monitored.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; system security plan; physical access logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for monitoring physical access; mechanisms supporting or implementing physical access monitoring; mechanisms supporting or implementing the review of physical access logs].

Testing Assessment Notes:

Maturity Level 3

Capability C028: Limit physical access

Practice PE.3.136: Enforce safeguarding measures for CUI at alternate work sites.

Discussion: [DRAFT NIST SP 800-171 R2]: Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

CMMC Clarification: Most organizations focus on securing their corporate network and devices. Today many organizations have mobile staff who work from home or travel as part of their job. This means the organization needs to define and implement safeguards to account for protection of information beyond the enterprise perimeter. Safeguards may include physical protections, such as locked file drawers, as well as electronic protections.

Example

In your organization many of the project managers work remotely as they often travel to sponsor locations or even work from home. Since the projects they work require access to Controlled Unclassified Information (CUI) the organization must ensure the same level of protection is afforded as when they work in the office. Each laptop is deployed with patch management and anti-virus software protection. Since data may be stored on the local hard drive you have enabled full-disk encryption on their laptops. When the remote staff member needs access to the internal network you require VPN connectivity that also disconnects the laptop from the remote network (i.e., prevents split tunneling). The VPN requires multifactor authentication to verify the user is who they claim to be.

Mapping

- NIST SP 800-53R4: PE-17
- NIST SP 800-171: 3.10.6
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Enforce safeguarding measures for CUI at alternate work sites.

NIST SP 800-171R2 Related Discussion: Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

Assessment

Assessment Objective(s): Determine if:

3.10.6[a] safeguarding measures for CUI are defined for alternate work sites.

3.10.6[b] safeguarding measures for CUI are enforced for alternate work sites.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for personnel; system security plan; list of safeguards required for alternate work sites; assessments of safeguards at alternate work sites; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel]

Testing Assessment Notes:

Maturity Level 2

Capability C029: Manage backups

Practice RE.2.137: Regularly perform and test data backups.

Discussion: [CMMC]: Backups are used to recover data in the event of a hardware or software failure. Backups should be performed regularly based on an organizational defined frequency. They should be tested regularly to ensure they are performing as expected.

CMMC Clarification: Back up your organizational data so you can recover it if a hardware failure, software failure, or malware infection occurs. You can schedule backups to run automatically or manually. Many operating systems include a built-in feature to perform data backups.

After you create a backup, it is important to test it on a regular basis. When you test a backup, verify that the operating system, applications, and data are intact and functional. If you test data backups regularly, you will be in a better position to recover systems and files more efficiently if a failure or infection occurs.

Example

You are responsible for IT in your organization. One of your jobs is to make sure you can restore data if a serious event happens, such as a disaster, a hard drive failure, or a software problem. You have a backup procedure in place where you back up all your data weekly on a backup server. You set this up to occur automatically each weekend because it takes a lot of resources to perform a backup. You verify your backups every month. This ensures that your data is correct. It also confirms that you can use the data if you need to recover your systems.

Mapping

- NIST SP 800-53R4: CP-9
- NIST SP 800-171:
- CIS: 10.1,10.3
- CSF: PR.IP-4

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C029: Manage backups

Practice RE.2.138: Protect the confidentiality of backup CUI at storage locations.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backedup information containing CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

CMMC Clarification: You protect the confidentiality of information to ensure that it remains private and unchanged. Methods to ensure confidentiality may include:

- encrypting files;
- managing who has access to the information;
- physically securing devices and media that contains CUI; and
- managing the use of information.

Storage locations for information are varied, and may include:

- external hard drives;
- USB flash drives;
- disc media (e.g., CD, DVD, Blu-Ray);
- Networked Attached Storage (NAS);
- cloud backup; and
- FTP, FTP Secure, SFTP.

Example

You are in charge of protecting CUI for the company. You need to protect the confidentiality of backup data. You encrypt all your CUI data as it is saved on an external hard drive. Only people who are on the contract can access the hard drive. You secure the external hard drive in a physical location accessible only to people with permission.

Mapping

- NIST SP 800-53R4: CP-9
- NIST SP 800-171: 3.8.9
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Protect the confidentiality of backup CUI at storage locations.

NIST SP 800-171R2 Related Discussion: Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backed-up information containing CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

Assessment

Assessment Objective(s): Determine if the confidentiality of backup CUI is protected at storage locations.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Procedures addressing system backup; system configuration settings and associated documentation; security plan; backup storage locations; system backup logs or records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with system backup responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for conducting system backups; mechanisms supporting or implementing system backups].

Testing Assessment Notes:

Maturity Level 3

Capability C029: Manage backups

Practice RE.3.139: Regularly perform complete, comprehensive, and resilient data backups, as organizationally defined.

Discussion: [CIS CONTROLS V7.1]: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted data. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine. This practice is based on the following CIS controls:

10.1 Ensure that all system data is automatically backed up on a regular basis.

10.2 Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

10.5 Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

CMMC Clarification: Ensure systems and data are backed up at an interval that enables an organization to restore the system or data in accordance with business requirements. A complete backup ensures that all of the files necessary to reconstruct a system are backed up. Comprehensive backups cover all of the systems defined by the organization as necessary for business effectiveness and/or continuity. You should complete the backups based on a regular schedule that satisfies the needs of your organization. Ensure that your backups are resilient to physical disaster and malicious attack (e.g., ransomware). One approach is to store at least one system backup off-site and offline to provide.

Example

You are in charge of IT operations for your organization. As part of your responsibilities, you manage the system that performs backups of your systems' data. You do this to meet the business objectives of your organization. Meeting these objectives will help you manage the loss of data, data availability, or the integrity of data in the event of a cyber-incident. For example, you may conduct incremental backups nightly and full system backups every Friday evening after business hours. You store your full system backups offline at a different location than your other systems. Doing this provides added protection of your backups from a cyber-event or physical disaster that may impact your organization.

Mapping

- NIST SP 800-53R4: CP-9, CP-9(3)
- NIST SP 800-171:
- CIS: 10.1,10.2,10.5

- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C030: Manage information security continuity

Practice RE.5.140: Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.

Discussion: [CMMC]: This practice is about information system resilience, and requires that the organization take the actions necessary to ensure that the information security components continue to operate as needed to achieve business success and to ensure that the system's part in protection of CUI is maintained. It should be noted that "as needed" and "the system's part" may change if, as a result of stress, contingency business operations are conducted; e.g., as part of the organization's continuity of operations (COOP) planning. Note that redundancy is typically an aspect of resilience, yet is seldom sufficient as the means for achieving needed resilience.

CMMC Clarification: This practice requires an organization to do what is needed in order for their cybersecurity solutions to continue to function under stress or attack. This means that even if a solution that helps protect the environment has a failure, then other mechanisms will fill in the gap in order for the functionality to continue. Redundant components can help with this as well as proper planning and implementation. If a firewall fails, make sure another firewall can take its place, or the environment should fail closed preventing traffic from passing until the problem can be fixed. By having redundancy in place, an organization may continue operations with confidence knowing their cyber security mission is functioning properly, and the components will continue to operate properly even when failures may be taking place.

Example 1

An environment has a log collection server in place for collecting end-point logs from across the enterprise. Knowing this could be a catastrophic problem if the log collection system goes down, the organization plans and creates a clone of the primary log server and has setup the environment to perform automated switch over in case the primary server goes down. This will allow the organization to continue to collect logs, perform analysis, and act on incidents that happen during the time the primary server is down.

Example 2

A proxy server that is used to protect an organization against malicious websites by utilization of website categorization is setup by the IT department. If this solution goes down, the company will need to shutoff communication to the Internet or allow people to browse websites without use of the categorization for protection. Loss of this protection mechanism could lead to malicious content being downloaded to user systems. The organization plans for secondary and tertiary proxies to be put in place and setup the solution so transfer of processing will occur in near real time if there is ever a problem with the primary. This not only allows continuity of operation for accessing Internet resources, but it also provides continuity of operations with respect to the protection provided by the proxy server's categorization capability.

Mapping

- NIST SP 800-53R4: CP-10
- NIST SP 800-171:
- CIS:
- CSF: PR.IP-9

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C031: Identify and evaluate risk

Practice RM.2.141: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or trans

Discussion: [DRAFT NIST SP 800-171 R2]: Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractor operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

NIST SP 800-30 provides guidance on conducting risk assessments.

CMMC Clarification: Risk arises from anything that can reduce an organization's assurance of mission/business success; cause harm to image or reputation; or harm individuals, other organizations, or the Nation.

Organizations should assess the risk to their operations and assets at regular intervals. Areas where weakness or vulnerabilities could lead to risk may include:

- poorly designed and executed business processes;
- inadvertent actions of people, such as disclosure or modification of information;
- intentional actions of people, such as insider threat and fraud;
- failure of systems to perform as intended;
- failures of technology; and
- external events, such as natural disasters, public infrastructure and supply chain failures.

An organization can perform a formal or an informal risk assessment. In a formal risk assessment, you use established criteria and procedures. Formal risk assessments are documented. It is important to note that risk assessments differ from vulnerability assessments (See RM.2.142). A vulnerability assessment provides input to a risk assessment along with other information such as results from likelihood analysis and analysis of potential treat sources.

Example

You help manage IT for your employer. You and your team members are working on a big government contract requiring you to store CUI. You assess the risk involved with storing CUI. You consider storing that information with a cloud provider. You and your coworkers discuss the pros and cons of this option. Then, you use these details to make the final decision about using a cloud provider.

Mapping

- NIST SP 800-53R4: RA-3
- NIST SP 800-171: 3.11.1
- CIS:
- CSF: ID.RA-1,ID.RA-4,DE.AE-4,RS.MI-3

NIST SP 800-171R2 Related Security Requirement: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or trans

NIST SP 800-171R2 Related Discussion: Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

Assessment

Assessment Objective(s): Determine if:

3.11.1[a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.

3.11.1[b] risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with risk assessment responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].

Testing Assessment Notes:

Maturity Level 2

Capability C031: Identify and evaluate risk

Practice RM.2.142: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

NIST SP 800-40 provides guidance on vulnerability management.

CMMC Clarification: A vulnerability scanner is an application that identifies an organization's asset vulnerabilities for which the scanner is capable of identifying. Then, the scanner creates a prioritized list of asset vulnerabilities ordered by their level of severity. The scanner also describes each vulnerability and the steps needed to fix it. Your organization should scan for vulnerabilities on all devices connected to the network. This includes servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers. All assets that have any form of connection to a wired network, Wi-Fi environment, and air-gapped labs that are associated with the CMMC assessment should be scanned.

Organizations that develop custom software should perform reviews of the software.

Vulnerability analysis of a custom-made solution requires an experienced penetration tester to properly test and validate findings. Automated vulnerability scanners do not necessarily perform well against custom developed applications.

The vulnerability scanning process should be a regular activity. It should not be a single occurrence. Organizations should put in place a vulnerability scanner that updates its database each time it performs a scan. This means that the scan looks for the most current vulnerabilities. Schedule scans with consideration of the potential for impact to normal operations. Use caution when scanning critical assets. These assets do need to be scanned, but some scanning options could cause a denial of service against a critical asset. You could replicate the critical asset in a test environment and perform vulnerability scans against the replicated asset. The replicated asset vulnerability scan will produce valid reports that need to be applied to the production system only if the replicated system is an exact duplicate of the production system and has identical functionality in operation when being tested.

Example

You are in charge of IT in your organization. You look for errors in your software that may provide ways for hackers to get into your network and do harm. You perform vulnerability scans to try and find these errors. You use a vulnerability scanner application that tests all the assets connected to your network. As a result of the scan, you get a prioritized list of vulnerabilities. Because you will scan everything connected to your network, you should set up the scan to happen at night. You should also make sure that your vulnerability scanner application gets updated on a regular basis.

Mapping

- NIST SP 800-53R4: RA-5
- NIST SP 800-171: 3.11.2
- CIS: 3.1,3.2
- CSF: ID.RA-1

NIST SP 800-171R2 Related Security Requirement: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

NIST SP 800-171R2 Related Discussion: Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

Assessment

Assessment Objective(s): Determine if:

3.11.2[a] the frequency to scan for vulnerabilities in organizational systems and applications is defined.

3.11.2[b] vulnerability scans are performed on organizational systems with the defined frequency.

3.11.2[c] vulnerability scans are performed on applications with the defined frequency.

3.11.2[d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified.

3.11.2[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or net

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].

Testing Assessment Notes:

Maturity Level 2

Capability C032: Manage risk

Practice RM.2.143: Remediate vulnerabilities in accordance with risk assessments.

Discussion: [DRAFT NIST SP 800-171 R2]: Vulnerabilities discovered, for example, via the scanning conducted in response to RM.2.142, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

CMMC Clarification: Review the prioritized list of vulnerabilities generated from the vulnerability scanner. Not all vulnerabilities may affect an organization the same. Review the risks of not remediating the discovered vulnerabilities. The organization should build upon the prioritized list and develop a prioritized mitigation plan for closing the vulnerabilities identified and track their completion.

Example

You are in charge of IT at your organization. Part of your job is to look for weaknesses in your software that may provide ways for hackers to get into your network and do harm. You perform vulnerability scans to try and find these weaknesses. The output of a scan is a list of the potential weaknesses, also called vulnerabilities. You should review the vulnerabilities and determine how they will affect your organization. You should create a prioritized list of the vulnerabilities you should fix, fix them, and record a completion date and time by each item. If you decide not to fix them, you should document the reasoning, and you should continue to monitor these vulnerabilities.

Mapping

- NIST SP 800-53R4: RA-5
- NIST SP 800-171: 3.11.3
- CIS: 3.7
- CSF: RS.MI-3

NIST SP 800-171R2 Related Security Requirement: Remediate vulnerabilities in accordance with risk assessments.

NIST SP 800-171R2 Related Discussion: Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

Assessment

Assessment Objective(s): Determine if:

3.11.3[a] vulnerabilities are identified.

3.11.3[b] vulnerabilities are remediated in accordance with risk assessments.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with informati

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].

Testing Assessment Notes:

Maturity Level 3

Capability C031: Identify and evaluate risk

Practice RM.3.144: Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

Discussion: [NIST CSF V1.1]: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

CMMC Clarification: This level 3 practice extends the related level 2 practice (RM.2.141) by requiring that defined risk categories, identified sources of risk, and specific risk measurement criteria be included in the risk assessment. Risk assessments are performed periodically to identify potential risks to the organization, or after an incident to mitigate recurrence of that risk. A risk assessment identifies risks to an organization's functions and the supporting assets: people, technology, information, and facilities. Threat information, vulnerabilities, likelihoods, and impacts are used to identify risk. Evaluate and prioritize the identified risks based on the defined risk criteria: risk sources, risk categories, and risk measurement criteria.

It is important to note that risk assessments differ from vulnerability scanning. A vulnerability scan focuses primarily on technical vulnerabilities in a system, and provides input to a risk assessment. A risk assessment may not be a strictly technical assessment. It includes such qualitative data as results from likelihood analysis and potential threat descriptions. Refer to RM.2.142 for vulnerability scanning.

Example

The CIO has asked you to perform a risk assessment for the organization’s IT assets. You assemble the leads from each major area across the IT organization. One of the first tasks the team performs is to define risk in terms of severity and impact to the organization. The team identifies organizational functions and the IT assets required to support them. This information is confirmed by executive input. You then lead the team through an exercise that defines the threats (e.g., APT, hacker, criminal) and attacker tools, techniques, and procedures (e.g., ransomware, defaced website) that the organization may face. The team uses publicly available information and previous internal IT assessments to create the organization’s threat list. The threats and an analysis of susceptibility are analyzed to determine the likelihood of occurring. The team ranks the impacts and prepares a report for the CIO. As a result of the report the CIO directs you to improve the security for the public facing web servers hosting a sponsor-used application. Additional tasks to mitigate risks are added to a prioritized action list to be worked by the IT organization.

Mapping

- NIST SP 800-53R4: RA-3
- NIST SP 800-171:
- CIS:
- CSF: ID.RA-5

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C032: Manage risk

Practice RM.3.146: Develop and implement risk mitigation plans.

Discussion: [CERT RMM V1.2]: When the consequences of risk exceed the organization's risk thresholds and are determined to be unacceptable, the organization must act to address risk to the extent possible.

Addressing risk requires the development of response strategies that may include a wide range of activities. In some cases, risk response will require adjustments to current strategies for protecting and sustaining assets and services. In other cases, the organization will find itself designing and implementing new controls and service continuity plans. In addition, because not all risk can be mitigated, the organization must be able to address residual risk—the risk that remains and is accepted by the organization after response plans are implemented. This risk must be analyzed and determined to be acceptable before the risk response plan is in place.

CMMC Clarification: For each identified risk, develop and implement a risk mitigation plan. Mitigation plans should define a risk disposition for each identified risk. Possible risk dispositions include: avoid, accept, monitor, defer, transfer, and mitigate. Mitigation plans define how to address or limit the identified risk. Risk mitigation plans may include:

- how the vulnerability or threat will be reduced;
- the actions that will limit risk exposure;
- controls to be implemented;
- staff responsible for the mitigation plan;
- the resources required for the plan;
- the implementation specifics (e.g., when, where, how); and • how the plan implementation will be measured or tracked.

Example

Having completed the risk assessment for your IT organization the CIO was presented with the risks to IT assets. As a result of the assessment report the CIO has asked you to develop plans to address specific risks (based on impact and likelihood). You setup a meeting with the lead for IT projects to discuss the assessment. During the meeting you are briefed on current IT activities in the organization. Using the assessment information and IT activities you develop an integrated list of IT activities and risk mitigations. The list defines a combined priority within the IT organization, proposed actions to reduce risk, who is responsible for completing the action, and the completion date.

Mapping

- NIST SP 800-53R4: PM-9
- NIST SP 800-171:
- CIS:

- CSF: ID.RA-6,ID.RM-1

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C032: Manage risk

Practice RM.3.147: Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.

Discussion: [CMMC]: Unsupported products are products that are no longer supported by the vendor. Typically they are at the end of their product life. When a product becomes unsupported, there are no security updates and patches, putting the system at an increased exposure to potential attacks. Manage unsupported products separately from your supported products with increased mitigations as necessary to reduce the risk to the organization arising from such exposure.

CMMC Clarification: In any organization technologies are introduced and removed from the environment. However, it may be necessary to continue using end-of-life technologies in support of a business or sponsor mission for extended periods of time. This timeline may extend well beyond the support offered by the vendor. When a vendor no longer supports your organization's products, they no longer provide critical software updates and security updates. This puts your organization at risk because vulnerabilities may remain unpatched. To mitigate these risks, you should manage unsupported products separately. The management of these products may include:

- determining risk exposure caused by unsupported products;
- identifying if extended support is available;
- isolating unsupported products within your organization's network (isolation techniques could include firewalls, VLAN separation, or air-gapped networks); and
- performing an upgrade, replacement, or retirement.

Example

You are in charge of IT operations at your organization. A system on your network has been identified as running an operating system that is over 10 years old. When you speak to the system owner she informs you that the system emulates a Department of Defense (DoD) platform that is still in the field. The system is needed to perform simulations and provide feedback to the sponsor. There is no funding to upgrade or replace the system. Additionally, the data processed is deemed Controlled Unclassified Information (CUI). While the system presents a risk to the network you understand the need to support business objectives. Since the system is old, no longer supported by the vendor, and cannot meet new cybersecurity requirements you recommend isolating the system. Working with the project manager you develop a plan to isolate the system to better protect the data and the overall organization.

Mapping

- NIST SP 800-53R4: SA-22(1)
- NIST SP 800-171:
- CIS: 2.2
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C031: Identify and evaluate risk

Practice RM.4.149: Catalog and periodically update threat profiles and adversary TTPs.

Discussion: [CMMC]: One method that more mature enterprises can use to protect its systems is to employ threat profiles and better understand adversary tools, techniques, and procedures (TTPs). This knowledge can be gained by threat feed information, training, and various frameworks available on the internet. By cataloging (or tracking) and updating threat profiles and adversary tools, techniques, and procedures, an organization can utilize this information when planning for enterprise updates, hunting for adversary activities on a network, and unraveling a complicated attack incident that may have taken place.

This information is a critical component when planning incident response actions, analyzing alerts on systems, and knowing the most likely asset an adversary is going to go after based on the TTPs they perform. When someone wants to win against an opponent, they typically study their opponent's techniques and tactics. This knowledge not only allows them to train properly for the event against that opponent, but it allows them to understand what the opponent is doing as well as what actions they're about to take based on knowledge of their past actions. This information helps an organization to gain a cyber-advantage over the adversary. The purpose of creating threat profiles and adversary TTPs is to help identify and gain knowledge about an adversary that is trying to cause harm to your enterprise. Adversary goals include: accessing an enterprise to steal credentials, accessing proprietary information, stealing technologies, and disrupting operations.

CMMC Clarification: This practice enables organizations to proactively increase their ability to include the adversary perspective in their cybersecurity planning and incident response. Organizations should know that setting up a security perimeter around their enterprise is no longer enough to keep that enterprise protected against the adversaries of today. Understanding the adversaries TTPs, and documenting how these techniques could be used against an organization is one of the first steps needed in order to keep the adversaries at bay. If an adversary gains access to an organization's enterprise, knowledge of their actions, what their standard operating procedures are, and what they may be going after can be a key part in eradicating them from your enterprise. See practice IR.4.100 for use of this information.

Example 1

Your organization has recently received information from a threat feed that adversaries are seeking technical knowledge in the area your company specializes. Your cyber defense team is put on high alert to look for actions that look out of the ordinary. In order to properly identify these actions, they look in their folder for activities related to the specific threat actor that has been identified. Now, these TTPs can be used to help the cyber defense team identify and eradicate actions taken by the adversary.

Example 2

Your organization wants to utilize knowledge of the adversaries to help plan and protect the organization against cyber-attacks. Your organization signs up for threat feed services that provide

updated information with respect to adversary TTPs. Your organization has individuals that receive this information and create a repository of threat profiles against your organization. These profiles are then used by various teams for planning cyber defenses for the organization. These same profiles are also used by the organizations Defensive Cyber Organization (DCO) to help monitor and protect the enterprise from adversary actions.

ADDITIONAL READING

National Council of ISACs: https://www.nationalisacs.org/

NSA/CSS Technical Cyber Threat Framework v2:

https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professionalresources/ctr-nsa-css-technical-cyber-threat-framework.pdf

ATT&CK: https://attack.mitre.org/

NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF: DE.AE-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C031: Identify and evaluate risk

Practice RM.4.150: Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.

Discussion: [DRAFT NIST SP 800-171B]: The constantly changing and increased sophistication of adversaries, especially the advanced persistent threat (APT), makes it more likely that adversaries can successfully compromise or breach organizational systems. Accordingly, threat intelligence can be integrated into and inform each step of the risk management process throughout the system development life cycle. This includes defining system security requirements, developing system and security architectures, selecting security solutions, monitoring (including threat hunting) and remediation efforts.

Support References:

- NIST SP 800-30 provides guidance on risk assessments.
- NIST SP 800-39 provides guidance on the risk management process.
- NIST SP 800-160-1 provides guidance on security architectures and systems security engineering.
- NIST SP 800-150 provides guidance on cyber threat information sharing.

CMMC Clarification: Threat intelligence (See RM.4.149 and SA.3.169) provides for an organization with a better understanding of the adversaries and their TTPs. This understanding helps an organization plan, design, architect, and integrate solutions in a manner that will help thwart adversary activities. This understanding should be used to design the enterprise architecture as well as the endpoint monitoring capabilities and to plan threat hunting actions. Threat intelligence can be very valuable when an organization is building their defensive playbook. Having defensive response and recovery actions planned prior to an attack taking place is key to having efficient and timely defensive cyber operation actions.

Practice IR.4.100 requires a similar use of adversary knowledge for incident response and execution.

Example 1

Your organization recently started subscribing to a threat feed service to gain valuable intelligence on adversary actions and what is currently happening against other organizations. Based on information gained from this service, your DCO team utilizes the information to hunt for adversary TTPs received from the service every day. This information helps provide up-to-date TTPs, and it also provide the latest adversarial actions taking place across other organizations subscribing to the threat feed, as well. This information is invaluable in molding your architecture towards specific threats as the information is received.

Example 2

Your new threat feed has recently sent out information that states a specific action against a specific vendor solution is underway at various organizations similar to your own. This information is passed to your DCO team for hunting operations, and the architecture team utilizes it to make small adjustments to the organizations enterprise architecture that prevents similar tactics from being successful in your environment.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF: ID.RA-2,ID.RA-3

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C031: Identify and evaluate risk

Practice RM.4.151: Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.

Discussion: [CMMC]: Adversaries constantly probe trusted boundaries, such as an organization's perimeter with the Internet, to find opportunities to create unauthorized connections. Organizations must perform their own scans to determine if unauthorized connections are possible. To help validate access control on network boundaries an organization will schedule actions, such as scanning from various points of presence to assets on various network segment boundaries to identify proper boundary access protections are in place and properly configured. This allows the organization to identify if there are trusted network boundaries that may be breached because of a misconfiguration, or due to the trust between one segment of an environment and another. Basically, this means a one-to-many connection attempt from each network boundary. Identifying the results of each test, where it was trying to access, whether it was successful or not, time of day, IP addresses, etc. can all be used to determine if the actions of the environment match the network protection design, i.e., whether an open port is authorized or unauthorized.

CMMC Clarification: Organizations need to perform actions to validate the implementation of the enterprise security architecture that restricts connections at trusted network boundaries. Mature organizations design, implement, document their security mechanisms, and they perform actions that help identify whether or not the security mechanisms are in place and working as expected. Even the best security practitioners have been known to make a slight mistake on a configuration of a security mechanism and find out later that the component is not providing the protection necessary to keep the environment secure.

Example 1

Your organization has a data center that only allows connectivity from clients over HTTPS web services. There is a firewall between the user network and the data center systems to make sure this access to controlled. The firewall admin mistakenly placed a rule into the system that allows a connection to HTTP services in the data center by users. This access may allow someone to access specific systems and send passwords over in the clear, thus exposing user credentials. Fortunately, a scan by corporate cyber services identifies this allowed connectivity and emails a report to the admin of the firewall. The admin changes the rule in the firewall and the access is stopped before anything bad happens.

Example 2

Your organization does not allow printers to initiate connectivity to any other environment within the enterprise. There is a firewall that prevents this action from taking place. Only user systems are allowed to initiate communication with printers. During routine checks, it is identified that the printer network has the ability to initiate communication to the user network as well as the data center. This could be bad if a printer becomes compromised. The firewall team is alerted of this finding and the problem is thwarted before communications are used in a manner undesired by the organization.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 12.2
- CSF: DE.CM-7

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C033: Manage supply chain risk

Practice RM.4.148: Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.

Discussion: [DRAFT NIST SP 800-171B]: The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase risk include the insertion or use of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking requiring a coordinated effort across an organization building trust relationships and communicating with both internal and external stakeholders. Supply chain risk management (SCRM) activities involve identifying and assessing risks, determining appropriate mitigating actions, developing SCRM plans to document selected mitigating actions, and monitoring performance against plans. SCRM plans address requirements for developing trustworthy secure and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes. NIST SP 800-161 provides guidance on supply chain risk management.

CMMC Clarification: An organization relies heavily on products and solutions created by other entities. These solution sets can add risk to an organization's overall cyber security posture. Organizations need to develop a plan for managing the supply chain risks associated with the IT supply chain. The scope of the plan is the IT suppliers for the networking, storage, and computing software, hardware, and services that support the storage, processing and transmission of CUI and are part of the CMMC assessment. This plan needs to be updated from time to time and verify that organization policies match the plan, and the organization follows this plan when obtaining solutions from this supply chain.

Example 1

The organization plans for managing supply chain risks with the IT supply chain, developing SCRM plan. As an example, the plan prohibits purchasing any products made in specific countries and requires that purchased items be tested in an offline environment prior to connecting them to the corporate network.

Example 2

An organization wants to purchase new laptops for a special project that will contain CUI. The purchasing process follows the supply chain risk management plan written by the organization. The laptops are purchased from a trusted vendor. After delivery the systems are analyzed for tampering and the BIOS compared with the version provided by the vendor. Once the systems pass these checks, then all of their operating systems are re-installed to prevent any unwanted software from being on the systems prior to given them to users.

Mapping

- NIST SP 800-53R4: SA-12
- NIST SP 800-171:
- CIS:
- CSF: ID.SC-1,ID.SC-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C032: Manage risk

Practice RM.5.152: Utilize an exception process for non-whitelisted software that includes mitigation techniques.

Discussion: [CMMC]: Whitelist technologies allow an organization to lock-down their environment in such a way that only allowed software will be able to run on end point and server systems. If a program is not listed on the whitelist, then it is not authorized to run on a given system.

While this may help keep organizations secure, it is not realistic to expect a stringent whitelist will meet all of the software needs. Most organizations of any size will need to create a process for expanding the whitelist quickly, or create an exception process that will allow individuals to get permission to run software that is needed for their job, but the organization does not want to globally accept that software running on all endpoints.

While whitelist technologies provide a method for organizations to choose which software packages can run in the overall enterprise, they require an organization to understand that some of the users will require software outside of the whitelist (non-whitelist) to be approved for use. A mature organization should have a procedure in place for determining what software is placed on the whitelist for the organization. At the same time, the organization should have a procedure for determining how software may run through an exception process. The exception process will determine what software needs to be authorized that is not within the whitelist. Part of this exception process may be a mitigation strategy, such as placing a given machine in a quarantine zone while it is using the software that is not whitelisted. Carefully controlling what software is authorized (whitelist) is a huge benefit to an organization, but this approach may require whitelist exceptions from time to time based on project and user needs. Having a well-defined process and documenting all steps for determining exceptions are key for demonstrating the maturity of the organization when determining what is safe and not safe to run on the enterprise environment.

An organization also needs to understand that each additional software package authorized to run on their environment adds a level of risk to the organization's enterprise.

CMMC Clarification: This practice defines and implements an explicit risk reduction process in the recognition that some software will be installed as an exception to the whitelist policy. Standard software packages that an organization trusts can easily be whitelisted based on risk and need for the organization. Once the whitelist is established, an organization needs to create a process that will allow software to be inspected and considered for operational use, even if only for a short period of time. If an operational need arises for a software package that adds too high of risk for the organization, the organization will need to decide if they will allow the software to run and under what circumstances. Mitigation strategies can be as extensive as only running software on a standalone system, or placing the software in a protected virtual machine with limited access to corporate assets. The list of acceptable mitigation strategies should be determined by the organization's cyber professional. When a user requests the right to use software that is not whitelisted, the organization should use their documented exception process to determine whether or not they are going to allow non-standard

software to be executed on endpoints. If the whitelist technology allows, an organization could associate exception software to a given asset on the enterprise. Another option could be placing the software inside a container and controlling what access it has on a system and on the enterprise.

Example 1

Your organization signs all executable software that runs on your endpoint Windows boxes. It is the signing cert that the whitelist software is looking for when accepting a software package to run. This not only makes it easier for the organization to add software to the list, but it is easier than adding software packages to the whitelist as the organization expands. A mechanical engineer needs to use a new CAD (computer aided design) software package that is not standard for the organization. The team does not want to sign it and make it standard across the enterprise. So, after analysis of the software, only the mechanical engineer's machine is authorized to run the software package. This allows the mechanical engineer to use it for their job function, but it prevents blanket coverage across the enterprise by refusing to sign the software to pass the corporate whitelist technology.

Example 2

Your medium size company has a whitelist technology installed on all end point systems. Being a good steward of cyber security, your company has all allowed software listed in the whitelist software. An HR representative needs to run a special software package to run reports against timesheets for auditors. You run the software through your vetting process, and don't find any negative issues with it. You add the software to the whitelist of the HR representative's system only so they can perform the report capability for the auditors.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C032: Manage risk

Practice RM.5.155: Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.

Discussion: [DRAFT NIST SP 800-171B]: Since sophisticated threats such as the APT are constantly changing, the threat awareness and risk assessment of the organization is dynamic, continuous and informs the actual system operations, the security requirements for the system, and the security solutions employed to meet those requirements. Threat intelligence (i.e., threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes) is infused into risk assessment processes and information security operations of the organization to identify any changes required to address the dynamic threat environment.

NIST SP 800-30 provides guidance on risk assessments.

CMMC Clarification: Organizations should perform regular assessments of their cybersecurity capability to include the effectiveness of the security controls in light of current threat intelligence. These assessments go beyond identifying misconfigurations and vulnerabilities to assessing the intended capability against newly acquired threat intelligence to determine if the expected effectiveness against the threat is still being achieved. Such an assessment could identify shortcomings in the intended cybersecurity capability that the adversary could take advantage of resulting in risks to the organization These assessments of the security solutions will help identify necessary changes in the design, architecture, and configuration of the solutions. These changes should be rolled into standard operating procedure timeframes and based on criticality of the findings.

Example 1

Your organization built a new service this year that will prevent users from browsing the internet directly. The new solution allows users to have indirect internet and allows downloaded content after a scrubbing and analysis process. During an assessment it was identified that this solution is working properly, except that all PDF files can be downloaded without being scrubbed and sent directly to the users' machines. This finding leads the team to look at the configuration of the solution and identify that a misconfiguration has been put in place. The team makes this finding a high priority and immediately put in a change request to the team that manages the solution. The assessment team works with the configuration team and verifies the change is put in place and PDFs are no longer downloaded without being analyzed.

Example 2

Your organization has end point protection on each enterprise user system. This solution helps monitor for malicious commands being run on the solution. During an assessment it is found that if a user attempts to run a music application that is already whitelisted, the end point monitoring solution fails. This causes an endpoint to lack the extra protection and monitoring desired by the organization. Upon

further analysis, it is identified the endpoints failing required a driver update to fix the problem. This problem was fixed and the endpoints no longer suffer from this issue.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 2

Capability C034: Develop and manage a system security plan

Practice CA.2.157: Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Discussion: [DRAFT NIST SP 800-171 R2]: System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

NIST SP 800-18 provides guidance on developing security plans.

CMMC Clarification: A system security plan (SSP) is a document that outlines how an organization implements its security requirements. An SSP outlines the roles and responsibilities of security personnel. It details the different security standards and guidelines that the organization follows. An SSP should include high-level diagrams that show how connected systems talk to each other. The organization should outline in its SSP its design philosophies. Design philosophies include defense-in-depth strategies as well as allowed interfaces and network protocols. All information in the SSP should be high-level. Include enough information in the plan to guide the design implementation of the organization's systems. Reference existing policies and procedures in the SSP.

Example

You are in charge of system security in your organization. As part of your job, you develop a system security plan (SSP). The SSP tells all employees how they can meet the organization's system security goals. The information in the SSP should explain how you should handle your important information. Examples include who can access important information, where you should store it, and how you can transmit it. By defining a clear SSP, you can design and build your network to ensure that it meets the SSP-defined goals. You can also use your SSP to outline the organization's:

- security requirements;

- the current status of the requirements; and
- your plan to meet the requirements in the future.

Mapping

- NIST SP 800-53R4: PL-2
- NIST SP 800-171: 3.12.4
- CIS:
- CSF: PR.IP-7

NIST SP 800-171R2 Related Security Requirement: Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

NIST SP 800-171R2 Related Discussion: System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls.

System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

Assessment

Assessment Objective(s): Determine if:

3.12.4[a] a system security plan is developed.

3.12.4[b] the system boundary is described and documented in the system security plan.

3.12.4[c] the system environment of operation is described and documented in the system security plan.

3.12.4[d] the security requirements identified and approved by the designated authority as non-applicable are identified.

3.12.4[e] the method of security requirement implementation is described and documented in the system security plan.

3.12.4[f] the relationship with or connection to other systems is described and documented in the system security plan.

3.12.4[g] the frequency to update the system security plan is defined.

3.12.4[h] system security plan is updated with the defined frequency.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

Testing Assessment Notes:

Maturity Level 2

Capability C035: Define and manage controls

Practice CA.2.158: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the system life cycle.

NIST SP 800-53 provides guidance on security and privacy controls for systems and organizations. SP 800-53A provides guidance on developing security assessment plans and conducting assessments.

CMMC Clarification: As organizations implement security controls, they should avoid a “set it and forget it” mentality. The security landscape is constantly changing. Reassess existing controls at periodic intervals in order to validate their usefulness in organizational systems. This will let you determine if the control is still meeting the needs of the organization. Set the assessment schedule according to organizational needs. Consider regulatory obligations and internal policies when assessing the controls.

Typical outputs of the practice include:

- documented assessment results;
- proposed new controls, or updates to existing controls;
- remediation plans; and
- new identified risks.

Example

You are in charge of IT operations in your company. You ensure that security controls are achieving their objectives. After you implement the controls, you monitor their performance. You should perform this review as often as necessary to meet:

- your organization's risk planning needs; and
- any regulations or policies you must follow.

When you assess the controls, document what you find. When you find your controls are not meeting your requirements, you should act and make changes. You can:

- propose updated or new controls;
- develop a plan to improve the control; and
- document new risks that you find.

You should also document these actions.

Mapping

- NIST SP 800-53R4: CA-2
- NIST SP 800-171: 3.12.1
- CIS:
- CSF: DE.DP-3

NIST SP 800-171R2 Related Security Requirement: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

NIST SP 800-171R2 Related Discussion: Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the system life cycle.

Assessment

Assessment Objective(s): Determine if:

3.12.1[a] the frequency of security control assessments is defined.

3.12.1[b] security controls are assessed with the defined frequency to determine if the controls are effective in their application.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with security assessment responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].

Testing Assessment Notes:

Maturity Level 2

Capability C035: Define and manage controls

Practice CA.2.159: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

CMMC Clarification: When you write a plan of action, you should define the clear goal or objective of the plan. You may include the following in the action plan:

- ownership of who is accountable for ensuring the plan's performance;
- specific steps or milestones that are clear and actionable;
- assigned responsibility for each step or milestone;
- milestones to measure plan progress; and
- completion dates.

Note that receiving Cybersecurity Maturity Model Certification requires all practices and processes to be implemented at the time of assessment. Any security requirements that were part of a plan of action must be closed/met in order to be granted the CMMC assessment.

Example 1

You are in charge of IT operations in your organization. Your job is to develop action plans when you discover that your company isn't meeting security requirements. One of your sources of information is the output of vulnerability scans on your network. When you receive notification of a vulnerability that needs fixing, you develop a plan to fix it. Your plan identifies the person responsible for fixing it, how to do it, and when to do it. You will also define how to measure that the person responsible has fixed the vulnerability. You document this in a plan of action.

Example 2

A company that is CMMC L1 compliant seeks L3 compliance. The IT department tracks the implementation of the additional security requirements needed for L3 in an action plan and realizes that it will be more than 6 months before CMMC L3 requirements can be met. Company officials refer to the

action plan that indicates that CMMC L2 requirements are currently met and decide to pursue CMMC L2 compliance instead of L3 and seek L3 certification next year.

Mapping

- NIST SP 800-53R4: CA-5
- NIST SP 800-171: 3.12.2
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

NIST SP 800-171R2 Related Discussion: The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Assessment

Assessment Objective(s): Determine if:

3.12.2[a] deficiencies and vulnerabilities to be addressed by the plan of action are identified.

3.12.2[b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

3.12.2[c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action].

Testing Assessment Notes:

Maturity Level 3

Capability C035: Define and manage controls

Practice CA.3.161: Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Discussion: [DRAFT NIST SP 800-171 R2]: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions. Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

CMMC Clarification: You should provide a plan for monitoring and assessing the state of security controls on a recurring basis that occurs more frequently than the periodic assessments discussed in CA.2.158. This process provides a mechanism to assess the overall security posture of your organization. As a result the process not only maintains awareness of vulnerabilities and threats, but also informs management of the effectiveness of the security controls in determining if security controls are current and for management to make an acceptable risk decision.

Example

As the lead for cybersecurity at your organization your boss has asked you to ensure that any requirements for cybersecurity are met. Since the organization supports Department of Defense (DoD) contracts you are aware that contractors must meet specific compliance requirements. You review those requirements and the associated preventative, detective, or responsive security controls you've implemented to identify any gaps. With your list of compliance requirements and actual security controls in place you create a plan of action to evaluate each control regularly over the next year. You mark several controls to be evaluated by a third party security assessor. After reviewing the list with several colleagues in IT you assign them responsibility to evaluate controls within their area of responsibility. The remaining controls are assigned to members of the IT cybersecurity team. To ensure progress you establish recurring meetings with the accountable IT staff to assess continuous monitoring progress, review security information, evaluate risks from gaps in continuous monitoring, and produce reports for your executives.

Mapping

- NIST SP 800-53R4: CA-7
- NIST SP 800-171: 3.12.3
- CIS:

- CSF: PR.IP-7,DE.DP-5

NIST SP 800-171R2 Related Security Requirement: Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

NIST SP 800-171R2 Related Discussion: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions.

Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

Assessment

Assessment Objective(s): Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Security planning policy; organizational procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

Testing Assessment Notes:

Maturity Level 3

Capability C036: Perform code reviews

Practice CA.3.162: Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.

Discussion: [CMMC]: Creating secure software implementations is difficult and requires extra steps to assess the code for security related vulnerabilities. Security assessment is a process of reviewing software source code in order to identify defects or vulnerabilities within an application. Security assessment may be done using manual or automated techniques.

CMMC Clarification: The purpose of the security assessment is to assure the organization that the code has undergone sufficient testing to identify and mitigate errors or vulnerabilities. The review can be performed using static and/or dynamic application security testing tools. Static analysis examines the source code before the program is run. Developers vet the code against a set of rules. By performing static analysis early in the development process the developer can identify specific errors and correct in a timely manner. Dynamic testing executes the code to identify potential execution, memory, and data issues in real-time. Manual code reviews use development teams to review the code against a set of secure development guidelines.

Example

You are in charge of IT operations for your organization. You have a group of developers who create internal software applications. Because you develop the software in house, you make sure the code is reviewed so that code mistakes do not result in vulnerabilities. You have another software engineer, who is not part of the development team, perform a manual code review to ensure the software meets standards set by the organization. You do this for each software update or iteration. You prohibit the software from being run on the organization's network until the code review is complete.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 18.1,18.2
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C034: Develop and manage a system security plan

Practice CA.4.163: Create, maintain, and leverage a security roadmap for improvement.

Discussion: [CMMC]: As organizations become more mature in their cyber security operations, it is expected that an organization will create, maintain, and leverage a security roadmap to show their planned path forward for improvements. This demonstrates a maturity level within an organization that is above the average company. The security roadmap will help a company move forward with increasing their overall security posture based on priority, cost, and implementation time. Such planning will help an organization line up vendors to discuss the planning and what solutions they may offer, receiving bids to help with the work, or get a bid on a cybersecurity appliance that will be installed on location or an "as a service" solution from a cloud provider that will be utilized remotely. This roadmap should be used to help plan based on areas of highest risk, latest TTPs, and or knowledge that a specific industry is being targeted and pushing solutions forward that will thwart malicious activities. A roadmap will require updates from time to time based on intelligence or architecture needs. A roadmap will survive people changing positions, and it will provide continuity plan for improving the cybersecurity posture of an organization.

CMMC Clarification: An organization must explicitly identify its desired end-state for cybersecurity capabilities and document a roadmap describing the planned path forward. Increasing measures along the way reduces the likelihood of a cyber-attack being successful or minimizes the impact of an attack. The roadmap should have short, medium, and long term goals for the organization. Plan for what the organization wants to accomplish in the next 6-12 months (short term). Also plan for 12-36 months (medium term), and plan for 5-10 years. All of the plans can be adjusted over time, but having the plans will allow for budgeting, priorities, and knowledge as to where to organization is going to keep the environment safe from adversaries.

Example 1

The organization sees its security end-state as being comparable to similar sized companies that are considered to have good cybersecurity capabilities. An immediate shortfall has been identified related to email coming into the organization without any filtering capabilities in place. This requires the organization to thwart email attacks at the endpoint and have additional controls on the enterprise to help thwart such attacks. The security roadmap outlines a plan to have automated spam filters, sandboxing of attachments, and link analysis in place within 6 months to help reduce the likelihood of an attack coming from email. Example 2

The organization has a VPN solution that does not require multifactor authentication (MFA). The security roadmap outlines a plan to have MFA in place within the next year, which will reduce the likelihood of remote attackers gaining access to the VPN through stolen credentials.

Mapping

- NIST SP 800-53R4: PL-1
- NIST SP 800-171:

- CIS:
- CSF: ID.RM-1,RS.IM-1,RS.IM-2,RC.IM-1,RC.IM-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C035: Define and manage controls

Practice CA.4.164: Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.

Discussion: [DRAFT NIST SP 800-171B (MODIFIED)]: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify weaknesses and vulnerabilities within the solution. Adversaries that obtain a foothold in a network can take advantage of any unpatched vulnerabilities. Penetration testing goes beyond automated vulnerability scanning, and the testing is conducted by penetration testing agents and teams with demonstrable skills and experience that includes technical expertise in network, operating system, and/or application level security. Penetration testing is used to validate vulnerabilities or determine the degree of penetration resistance of systems to cyber-attacks. The resistance to attacks is similar to withstanding an adversary, but with constraints. Such constraints include time, resources, and skills. Penetration testing activities can receive support by utilizing automated vulnerability identification tools that are commercially available. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and should exercise both physical and technical controls, where possible. A standard method for penetration testing includes pretest analysis based on full knowledge of the system; pretest identification of potential vulnerabilities based on pretest analysis; and testing designed to determine exploitability of vulnerabilities. All parties agree to the rules of engagement before commencement of penetration testing scenarios. Organizations correlate the rules of engagement for penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. The penetration testing team may be organization-based or external to the organization. In either case, it is important that the team possesses the necessary skills and resources to do the job and is objective in its assessment. The findings from the penetration testing should be placed in a final report. Any and all findings need to be rolled into a prioritized security plan based on risk, cost, and time to implement.

NIST SP 800-53A provides guidance on conducting security assessments.

CMMC Clarification: This practice focuses on performing penetration testing (pentesting) against organizational solutions in order to identify vulnerabilities and weaknesses. Pentesting is a crucial component to help identify vulnerabilities in solutions as well as help identify flaws in systems under development and production systems. By performing penetration testing an organization can utilize the findings as feedback for development teams to utilize while planning system patching and mitigation strategies. Pentesting teams should have full access to documentation and source code (if developed in-house) of the solutions being tested prior to running attacks. An adversary will attempt to gain full knowledge about a system prior to attacking it; this will increase their likelihood of success. The adversary does this over a period of time, which includes research, recon, and gaining an understanding about the solution prior to launching an attack. The organization should allow a pentest team to have full knowledge of the solution prior to attacking it in order to perform better vulnerability analysis against it. The findings from the pentesting team effort should be used to help build mitigation plans for the solution, which may include modification to source code, design changes, as well as architecture

changes. Overall, pentesting should help identify issues that should be fixed in order to increase the overall security posture of the solution.

Penetration testing can be performed by an in-house team or a trusted third party. Penetration testing of different adversary types should be conducted over time.

Example 1

You are the CISO of an organization that has experienced pentesters and you utilize them to identify vulnerabilities in internal systems, report the findings, and have the system owners prioritize fixing problems that were identified during the testing. You have this penetration test team perform tests against various organizational assets on a round robin basis over the course of one year. This will allow the organization to perform pentesting on solutions at least annually, and the owners are expected to take the findings and implement mitigations before the next test period.

Example 2

You are the CISO of a small organization that lacks team members experienced in pentesting, but you want to perform this practice. You realize hiring fulltime team members with the penetration testing experience needed is going to be expensive for what will amount to a few weeks of testing a year. You seek out the help of an experienced pentesting organization and have them perform testing several times a year at a fraction of the cost of hiring someone. The information they provide is thorough, and you utilize it to mold your mitigation plans and security planning. The pentesting reports are your evidence this practice is performed.

Mapping

- NIST SP 800-53R4: CA-8
- NIST SP 800-171:
- CIS: 20.2
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C035: Define and manage controls

Practice CA.4.227: Periodically perform red teaming against organizational assets in order to validate defensive capabilities.

Discussion: [CMMC]: Red Teaming is a specialized type of assessment conducted against an organization's architecture with the goal to emulate adversary actions. This practice is focused on performing red teaming for the purpose of validating defensive capabilities in place (access controls, email protections, network segmentation, firewalls, and the defensive tools that help monitor all activities). It is recommended that red teaming events be coordinated with the defensive cyber teams of an organization in order to validate defensive cyber capabilities. This testing will help shape where defensive resources are allocated and where funding is needed to improve the overall security posture of the organization. This activity includes some vulnerability analysis, similar to a pentesting effort, but the main purpose is to validate defensive security mechanisms are providing the information needed to identify, disrupt, or thwart attacks on the network. Any and all findings need to be rolled into a prioritized security plan based on risk, cost, and time to implement.

CMMC Clarification: This practice focuses on red teaming an organization for the purpose of validating defensive cyber capabilities focusing on identifying or thwarting attacks. As the red team performs tests against the organization the red team is also working with the organization's cyber defender(s) in order to help validate the defensive capabilities against the attacks used. This is a completely transparent relationship where the red team works with the organization's cyber defenders in order to identify areas that need improvement. While large corporations may have internal teams perform this testing, a lot of small companies will lack the in-house expertise to perform red teaming properly. Third-party adversarial assessment teams can be used in this case. Rules of engagement will need to be generated prior to testing in order to define the bounds of the testing, and to make sure test teams know to what levels they may perform testing and making sure the in-bound assets are defined. The red team and cyber defense teams need to keep in mind that they are working together to find gaps, identify misconfigurations, and help improve the cyber defenses of the organization.

Red teams are typically asked to test environments from outside the enterprise and work their way in. It is recommended to allow red teams to perform testing from inside the environment as well, acting as if the outer perimeter protections have been breached, even if they are considered secure. The best results will be achieved when the red team is given the architectural knowledge of the environment being tested. When completed, the organization should have a better understanding of any cyber defense shortfalls, and be able to prioritize implementing changes as needed.

Example 1

You are the CISO for an organization and want to make sure your new endpoint tools are working to provide your defensive cyber operations with the information they need to identify an attack. You have an internal red team that performs several no notice attacks on a select few end user laptops. You find out that two out of three attacks are identified from capabilities already in place. You also learn that the third attack is successful and your DCO team is not provided enough information to determine it

happened. You ask your security engineers to modify the configuration of the tool and have your red team rerun the tests. Your DCO now can identify the third attack, and they are based on the latest TTPs provided by your intelligence service. You are now confident in your team's ability to see actions of this nature and trust your DCO team will identify them if they occur.

Example 2

You are the CISO of a small organization and want to hire a red team to help test your security solutions in place. You find a well suited commercial company to provide you red team services. You have them perform their testing three times a year to validate your DCO team is able to identify specific attacks based on threat intelligence feeds your organization is currently receiving. The commercial red team is introduced to your defensive cyber folks and they plan the tests and start working on identifying any shortfalls in defensive cyber operations. The red team provides you a report at the end of each test phase and you use the report to plan and implement modification to your security posture for enhancement purposes.

Mapping

- NIST SP 800-53R4: CA-8(2)
- NIST SP 800-171:
- CIS: 20.3
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C037: Implement threat monitoring

Practice SA.3.169: Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.

Discussion: [CMMC]: Establish relationships with external organizations to gather cyber threat intelligence information. Cyber threat information from external sources should inform situational awareness activities within the organization. Relevant external threat information is communicated to stakeholders within the organization for appropriate action if needed.

CMMC Clarification: To enhance situational awareness activities within the organization, leverage external sources for cybersecurity threat information. Establish a relationship with external organizations, or periodically survey relevant sources, to ensure you are receiving up-todate threat intelligence information pertinent to your organization. Examples of sources include: US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, and federal briefings.

Threat information is reviewed and, if applicable to your organization, communicated to the appropriate stakeholders for action.

Example

You are in charge of IT operations for your company. Part of your role is to ensure you are aware of up-to-date cyber threat intelligence information so you can properly perform risk assessments and vulnerability analyses. To do this, you join a defense sector ISAC, and signup for alerts from US-CERT. You use information you receive from these external entities to update your threat profiles, vulnerability scans, and risk assessments. Also, you use these sources to gather best practices for informing your employees of potential threats and disseminate the information throughout your organization to the appropriate stakeholders.

Mapping

- NIST SP 800-53R4: PM-16
- NIST SP 800-171:
- CIS:
- CSF: ID.RA-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C037: Implement threat monitoring

Practice SA.4.171: Establish and maintain a cyber-threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.

Discussion: [DRAFT NIST SP 800-171B]: Threat hunting is an active means of cyber defense in contrast to the traditional protection measures such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management (SIEM) technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indicators of compromise are forensic artifacts from intrusions that are identified on organizational systems at the host or network level, and can include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams use existing threat intelligence and may create new threat information, which may be shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies. Threat indicators, signatures, tactics, techniques, and procedures, and other indicators of compromise may be available via government and non-government cooperatives including Forum of Incident Response and Security Teams, United States Computer Emergency Readiness Team, Defense Industrial Base Cybersecurity Information Sharing Program, and CERT Coordination Center.

Support References:

- NIST SP 800-30 provides guidance on threat and risk assessments, risk analyses, and risk modeling.
- NIST SP 800-160-2 provides guidance on systems security engineering and cyber resiliency.
- NIST SP 800-150 provides guidance on cyber threat information sharing.

CMMC Clarification: In the cyber arena of today, adversaries are increasingly successful at getting into networks and maintaining their access. Adversaries may be in your network from an attack that happened years ago. In order to find adversaries in an enterprise an organization must perform hunting for the latest TTPs used by the adversaries. In order to do this an organization stands up a threat hunting team or contracts for one that uses a variety of methods, such as log analysis, network traffic analysis, and threat intelligence in order to look for indications that adversaries have been on a system (and may continue to be in place). Once found, the threat hunting team must act quickly to remove the problem, report the incident up the command chain, and continue to look for other pieces of evidence that an adversary has been within the environment. After an incident is handled, then the team should create indicators from what they learned and provide it back to the community in order for others to benefit from the threat intelligence provided. This information could be as simple as a file hash, IP address of the command and control server, a domain name, or the actions that have happened on a system. All of these items can be rolled into an indicator sharing component for others to ingest and benefit.

Example 1

Your organization's cyber hunt team has noticed that bandwidth consumption at night has spiked in the last few weeks and recognizes that this may indicate the presence of a cyber adversary in the system. The hunt team takes advantage of all information available to them in order to determine why bandwidth utilization at night has spiked. The team uses threat intelligence about certain adversaries that perform exfiltration from networks. The team searches through event and security logs to identify a specific piece of software running on a system in a lab. They discover that the last person to use the system was a lab technician who installed software on the system. This software was malicious, allowing the adversary to access network files and perform exfiltration of information over the last few weeks. The team quickly takes the system offline for analysis and identifies another system running the same software. All impacted systems are taken offline for further analysis and the adversary has been removed from the network.

Example 2

Your organization receives user complaints that their laptops are not able to access the network. The information provided shows that the laptops are not connecting to resources to provide them access. The hunt team utilizes threat intelligence that states certain threats have been placing fake access points near organizations like yours in order to trick their systems into connecting and attempting to perform an attack against the systems. The hunt team utilizes this information to find fake access points within the area. Your organization creates a new policy pushing "authorized" access point information to the user systems. All offline systems are collected and provided this information, too. This prevents corporate machines from accessing fake access points.

Mapping

- NIST SP 800-53R4: PM-16
- NIST SP 800-171:
- CIS:
- CSF: DE.CM-1,DE.CM-2,DE.CM-3,DE.CM-4,DE.CM-5,DE.CM-6,DE.CM.7,DE.CM-8

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C037: Implement threat monitoring

Practice SA.4.173: Design network and system security capabilities to leverage, integrate, and share indicators of compromise.

Discussion: [CMMC]: Sharing IoCs (Indicators of Compromise) to systems across an enterprise strengthens an organization's ability to thwart adversaries. Designing an organization's security architecture to integrate and share IoCs rapidly increases the likelihood of stopping an attack that is happening at machine speed. Machine speed attacks are attacks that are happening in real-time and use automation to increase the speed at which the attack spreads and performs actions. Effective sharing requires that intelligence services as well as internal resources process IoC information and provide it to the necessary systems in order to act on the information quickly.

CMMC Clarification: Most cyber-defense solutions provide an API (Application Programming Interface) that allows an organization to automate updates to solutions for IoC blocking, hunting, or other mitigation. By automating the process, the organization will remove the likelihood of a human mistyping an entry, and it greatly reduces the time for insertion into the security solution as compared to manual entry.

Example 1

Your organization uses a cyber intelligence service and as information comes in, bad domains are provided that an organization would not want their assets visiting. Once received, the information is pushed to the corporate firewall, proxy server, and DNS services for blocking, and reducing the gap between receiving the information and the time it takes to block any access to the bad domains. This stops users from accessing potentially malicious files from the domains provided.

Example 2

The organization receives information that a specific attack probe is being launched from a foreign system. The threat report identifies the country codes and IP structure for the attack machines. Your intelligence processing solution collects this information and then adds the IP addresses to the block list of your corporate firewall. Within ten minutes after the automated process updated the firewall you receive logs of the attempts against the corporate website. The logs show the attempt but the details show the attempts were blocked. All of this took place without human intervention and prevented the attack from being successful.

Mapping

- NIST SP 800-53R4: SI-4(24)
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 1

Capability C039: Control communications at system boundaries

Practice SC.1.175: 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 information systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

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

CMMC Clarification: Just as your office or plant has fences and locks for protection from the outside, and uses badges and keycards to keep non-employees out, your company's IT network or system has boundaries that must be protected. Many companies use a web proxy and a firewall.

Web Proxy

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.

Firewall

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.

If your company is large enough, you might want to monitor, control, or protect one part of the company enterprise/network from the other. This can also be done with a firewall. You may want to do this to stop adversaries, hackers, or disgruntled employees from entering your network and causing damage.

Example

You are setting up the new network for your company, and want to keep the company's information and resources safe. You make sure to buy a router—a hardware device that routes data from a local area network (LAN) to another network connection—with a builtin firewall, then configure it to limit access to trustworthy sites. Some of your coworkers complain that they cannot get onto to certain websites. You explain that the new network blocks websites that are known for spreading malware.

Mapping

- NIST SP 800-53R4: SC-7
- NIST SP 800-171: 3.13.1
- CIS:
- CSF: PR.PT-4

NIST SP 800-171R2 Related Security Requirement: Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

NIST SP 800-171R2 Related Discussion: 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.

Assessment

Assessment Objective(s): Determine if:

3.13.1[a] the external system boundary is defined.

3.13.1[b] key internal system boundaries are defined.

3.13.1[c] communications are monitored at the external system boundary.

3.13.1[d] communications are monitored at key internal boundaries.

3.13.1[e] communications are controlled at the external system boundary.

3.13.1[f] communications are controlled at key internal boundaries.

3.13.1[g] communications are protected at the external system boundary.

3.13.1[h] communications are protected at key internal boundaries.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing boundary protection capability].

Testing Assessment Notes:

SC: System and Communications Protection C039:SC.1.176

Maturity Level 1

Capability C039: Control communications at system boundaries

Practice SC.1.176: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Discussion: [DRAFT NIST SP 800-171 R2]: Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloudbased technologies.

NIST SP 800-41 provides guidance on firewalls and firewall policy. SP 800-125B provides guidance on security for virtualization technologies.

CMMC Clarification: Separate the publicly accessible systems from the internal systems that need to be protected. Do not place the internal systems on the same network as the publicly accessible systems.

A network or part of a network that is separated (sometimes physically) from an internal network is called a demilitarized zone (DMZ). A DMZ is a host or part of a network put in a “neutral zone” between an organization’s internal network (the protected side) and a larger network, like the internet. To separate a subnetwork physically, your company may put in boundary control devices (i.e., routers, gateways, firewalls). This can also be done on a cloud network that can be separated from the rest of the network.

A DMZ can add an extra layer of security to your company’s LAN, because an external network node can reach only what is permitted to be accessed in the DMZ.

Physical separation might involve a separate network infrastructure, dedicated network equipment with separate LAN segments and a firewall between the internal network and the DMZ segment and a firewall between the DMZ segment and the internet. A logical separation might involve VLAN separation for the DMZ supporting a separate subnet with routing and access controls between subnets.

Example

The head of recruiting wants to launch a website to post job openings and allow the public to download an application form. After some discussion, your team realizes it needs to use a router and firewall to create a DMZ to do this. You host the server separately from the company’s internal network, and make sure the network has the correct security firewall rules. Your company gets a lot of great candidates for the open jobs, and the company’s internal network is protected.

Mapping

- NIST SP 800-53R4: SC-7
- NIST SP 800-171: 3.13.5
- CIS: 14.1
- CSF: PR.AC-5

NIST SP 800-171R2 Related Security Requirement: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

NIST SP 800-171R2 Related Discussion: 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. [SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

Assessment

Assessment Objective(s): Determine if:

3.13.5[a] publicly accessible system components are identified.

3.13.5[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing boundary protection capability].

Testing Assessment Notes:

Maturity Level 2

Capability C038: Define security requirements for systems and communications

Practice SC.2.178: Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Discussion: [DRAFT NIST SP 800-171 R2]: Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

CMMC Clarification: You should configure collaborative computing devices so they cannot be activated remotely. Examples of such devices are cameras, microphones, etc. All users should receive a notification when a collaborative computing device is in use. Notification can include an indicator light that turns on when in use, or a specific text window that appears on screen. If a device does not have the means to alert a user when in use, the organization should provide manual means. Manual means can include, as necessary:

- paper notification on entryways; and
- locking entryways when a collaborative computing device is in use.

Example

You are responsible for IT operations in your organization. Your organization has a group of remote employees who collaborate using cameras and microphones attached to their computers. You want to prevent the misuse of these devices. You disable the ability to turn on cameras or microphones remotely on all devices. You also use a tool to alert users when their cameras or microphones are turned on. Although remote activation is blocked, this enables them to see if the devices were activated remotely. By doing this, you reduce the likelihood of someone being able to turn these devices on and listen or view what your employees are working on.

Mapping

- NIST SP 800-53R4: SC-15
- NIST SP 800-171: 3.13.12
- CIS:
- CSF: PR.AC-3

NIST SP 800-171R2 Related Security Requirement: Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

NIST SP 800-171R2 Related Discussion: Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

Assessment

Assessment Objective(s): Determine if:

3.13.12[a] collaborative computing devices are identified.

3.13.12[b] collaborative computing devices provide indication to users of devices in use.

3.13.12[c] remote activation of collaborative computing devices is prohibited.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for managing collaborative computing devices].

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting or implementing management of remote activation of collaborative computing devices; mechanisms providing an indication of use of collaborative computing devices].

Testing Assessment Notes:

SC: System and Communications Protection C038:SC.2.179

Maturity Level 2

Capability C038: Define security requirements for systems and communications

Practice SC.2.179: Use encrypted sessions for the management of network devices.

Discussion: [CMMC]: Management of network devices is a security critical process and needs to have confidentiality protection and authentication to protect against adversaries trying to gain information or change the network infrastructure.

Confidentiality protection prevents an adversary from sniffing passwords or configuration information. Authenticity protection includes, for example, protecting against man-in-themiddle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services).

CMMC Clarification: When an organization connects to and manages network devices, it should use an encrypted session. The most common encrypted method is a Secure Shell (SSH).

Example

You are an IT administrator for your organization. You are in charge of updating devices on your network. You access these devices over the network instead of at the device's physical location. When you establish a connection to these devices, you use an SSH connection. An SSH connection protects you. For example, an adversary has installed malware on a network device. If you use an unencrypted session (i.e., telnet into a device) the adversary can view your username and password. But, if you use an SSH connection, the adversary cannot see this information.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 11.5
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.177: Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Discussion: [DRAFT NIST SP 800-171 R2]: Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography.

CMMC Clarification: Only use FIPS-validated cryptography to protect the confidentiality of CUI since it has been tested and validated to meet FIPS 140-3 requirements. Any other cryptography cannot be used since it has not been tested and validated to protect CUI. FIPS validated cryptography is not a requirement for all information, FIPS-validation is only used for the protection of CUI.

Example

You are an IT administrator responsible for deploying encryption on all devices that contain CUI for your organization. You must ensure that the encryption you use on the devices is FIPS validated cryptography. An employee informs you that they must carry a large volume of CUI offsite and asks for guidance on how to do so.

You provide the user with Whole Disk Encryption software that you have verified via the NIST website uses a FIPS 140-3 validated encryption module. You instruct the user on the use of the software. Once the encryption software is active, the user copies their CUI data onto the drive to transport the data.

Mapping

- NIST SP 800-53R4: SC-13
- NIST SP 800-171: 3.13.11
- CIS: 14.4,14.8
- CSF: PR.DS-1,PR.DS-2

NIST SP 800-171R2 Related Security Requirement: Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

NIST SP 800-171R2 Related Discussion: Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPSvalidated cryptography and/or NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; and [NIST CMVP].

Assessment

Assessment Objective(s): Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing cryptographic protection; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting or implementing cryptographic protection].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.180: Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

CMMC Clarification: Familiarity with security engineering principles and their successful application to your infrastructure will increase the security of your environment. NIST SP 800-160 System Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems can serve as a source of security engineering and design principles.

Organizations need to decide which designs and principles to apply. Some will not be possible or appropriate for your organization as a whole. Some will not be possible, applicable, or appropriate for specific systems or components.

Once a decision is made on which designs and principles to apply, they should be applied to your organization's policies and security standards. Starting with your baseline configuration, they should be extended through all layers of the technology stack (e.g., hardware, software, firmware) and throughout all the components of your infrastructure. The application of these chosen designs and principles should drive your organization towards a secure architecture with the required security capabilities and intrinsic behaviors present throughout the lifecycle of your technology.

As legacy components in your architecture age, it may become increasingly difficult for those components to meet security principles and requirements. This should factor into life-cycle decisions for those components (e.g., replacing legacy hardware, upgrading or re-writing software, upgrading run-time environments).

Example

You are the security architect responsible for developing strategies to protect data and harden your organization's infrastructure. You are included on the team responsible for performing a major upgrade on a legacy system. You refer to the company's documented security engineering principles. Reviewing each, you decide which are appropriate and applicable. You apply the chosen designs and principles when creating your design for the upgrade.

You document the security requirements for the software and hardware changes to ensure the principles are followed. You review the upgrade at critical points in the workflow to ensure the requirements are met. You assist in updating the policies covering the use of the upgraded system so user behavior stays aligned with the principles.

Mapping

- NIST SP 800-53R4: SA-8
- NIST SP 800-171: 3.13.2
- CIS: 5.1,5.2,5.4
- CSF:

NIST SP 800-171R2 Related Security Requirement: Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

NIST SP 800-171R2 Related Discussion: Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

Assessment

Assessment Objective(s): Determine if:

3.13.2[a] architectural designs that promote effective information security are identified.

3.13.2[b] software development techniques that promote effective information security are identified.

3.13.2[c] systems engineering principles that promote effective information security are identified.

3.13.2[d] identified architectural designs that promote effective information security are employed.

3.13.2[e] identified software development techniques that promote effective information security are employed.

3.13.2[f] identified systems engineering principles that promote effective information security are employed.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; system and communications protection policy; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; security architecture documentation; security requirements and specifications for the system; system design documentation; system configuration settings and associated documentation; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with responsibility for determining information system

Interview Assessment Notes:

Test: [SELECT FROM: Separation of user functionality from system management functionality].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.181: Separate user functionality from system management functionality.

Discussion: [DRAFT NIST SP 800-171 R2]: System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

CMMC Clarification: Prevent user functionality and services from accessing system management functionality on IT components, e.g., databases, network components, workstations, servers. This reduces the attack surface to those critical interfaces by limiting who can access them and how they can be accessed. This can be achieved through both logical and physical methods using computers, CPUs, operating system, network addresses or a combination of these methods. By separating the user functionality from system management functionality, the administrator or privileged functions are not available to the general user.

The intent of this practice is to ensure:

- general users are not permitted to perform system adminstation functions; and
- system administrators only perform system administration functions from their privileged account.

This can be accomplished using separation like VLANs or logical separation using strong access control methods.

Example 1

You are an IT administrator responsible for preventing access to information system management functions for your organization. Your company has a policy stating that system management functionality must be separated from user functionality.

To comply with the policy, you provide physical protection by segregating certain functions to separate servers and connect those servers to their own sub-net network. You limit access to the separate servers so only approved system administrators can access them. They use special admin accounts with a different username from their normal accounts to login to these servers.

Example 2

You are an IT administrator responsible for preventing access to information system management functions for your organization. Your company has a policy stating that system management functionality must be separated from user functionality.

You login to the servers using a standard account to perform your daily work. Occasionally, you need to perform administrative tasks. To perform those tasks, you enter a command that elevates your rights to a system administrator. You enter your administrator credentials, which are different from your daily user account, to execute the administrative tasks. When completed, you go back to using your standard account.

Mapping

- NIST SP 800-53R4: SC-2
- NIST SP 800-171: 3.13.3
- CIS: 4.3
- CSF:

NIST SP 800-171R2 Related Security Requirement: Separate user functionality from system management functionality.

NIST SP 800-171R2 Related Discussion: System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

Assessment

Assessment Objective(s): Determine if:

3.13.3[a] user functionality is identified.

3.13.3[b] system management functionality is identified.

3.13.3[c] user functionality is separated from system management functionality.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Separation of user functionality from system management functionality].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.182: Prevent unauthorized and unintended information transfer via shared system resources.

Discussion: [DRAFT NIST SP 800-171 R2]: The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

CMMC Clarification: No shared system resource such as cache memory, hard disks, registers, or main memory should be able to pass information from one user to another user. In other words, when objects are reused no residual information should exist on that object. This protects the confidentiality of the information. This is typically a feature provided by operating system and software vendors.

Example

You are the system administrator for your company. You are creating the system hardening procedures for your company's computers. To prevent unauthorized and unintended information transfer via shared resources, you include in your procedures steps to verify the operating system is configured correctly. You examine the Computer Configuration policies in the operating system and verify the settings match those documented in the hardening procedures.

Mapping

- NIST SP 800-53R4: SC-4
- NIST SP 800-171: 3.13.4
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Prevent unauthorized and unintended information transfer via shared system resources.

NIST SP 800-171R2 Related Discussion: The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This

requirement also applies to encrypted representations of information. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Assessment

Assessment Objective(s): Determine if unauthorized and unintended information transfer via shared system resources is prevented.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system security plan; system design documentation; system

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing boundary protection capability].

Testing Assessment Notes:

SC: System and Communications Protection C038:SC.3.183

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.183: Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

CMMC Clarification: Block all traffic going into and coming out of the network, but permit specific traffic into and coming out based on the organization's policies, exceptions, or criteria. This process of permitting only authorized traffic to the network is called whitelisting which limits the number of unintentional connections to the network.

Example

You are the IT administrator setting up a new environment to house the company's CUI. You install firewalls between this environment and the other networks of the company with firewall rules that deny all traffic. You go through each service and application that runs in the new environment and only allow the required ports and network paths to be opened. You test the functionality of the required services and applications to make sure they work. You comment each firewall rule so there is documentation why it is required.

You review the firewall rules on a regular basis to make sure there were no unauthorized changes made (e.g., during troubleshooting of networking issues).

Mapping

- NIST SP 800-53R4: SC-7(5)
- NIST SP 800-171: 3.13.6
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

NIST SP 800-171R2 Related Discussion: This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

Assessment

Assessment Objective(s): Determine if:

3.13.6[a] network communications traffic is denied by default.

3.13.6[b] network communications traffic is allowed by exception.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing traffic management at managed interfaces].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.184: Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Discussion: [DRAFT NIST SP 800-171 R2]: Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

CMMC Clarification: Split tunneling for a remote user utilizes two connections: accessing resources on the organization's network via a VPN and simultaneously accessing an external network such as the public network or the Internet. Split tunneling introduces a vulnerability where an open unencrypted connection from the public network could allow an adversary to access resources on the network. As a mitigation strategy, the split tunneling setting should be disabled on all devices so that all traffic, including traffic for external networks or the Internet, goes through the organization's VPN.

Example

You are an IT administrator at your organization responsible for configuring the network to disallow remote users from using split tunneling. You perform a review of the configuration of remote user laptops. You discover that remote users are able to access files, email, database and other services through the organization's VPN connection. At the same time, remote users are able to access resources on the Internet through their connection to the Internet. You change the hardening procedures for the company's laptops to include changing the configuration setting to disable split tunneling. You test a laptop that has had the new hardening procedures applied and verify that all traffic from the laptop is now routed through the VPN connection.

Mapping

- NIST SP 800-53R4: SC-7(7)
- NIST SP 800-171: 3.13.7
- CIS: 12.12
- CSF: PR.AC-3

NIST SP 800-171R2 Related Security Requirement: Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

NIST SP 800-171R2 Related Discussion: Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

Assessment

Assessment Objective(s): Determine if remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms implementing boundary protection capability; mechanisms supporting or restricting non-remote connections].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.185: Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to internal and external networks and any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of the controls for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted.

CMMC Clarification: Only use FIPS-validated cryptography to protect the confidentiality of CUI during transmission since it has been tested and validated to meet FIPS 140-3 requirements. Any other approved cryptography cannot be used since it has not been tested and validated to protect CUI. FIPS-validated cryptography is not a requirement for all information, it is only used for the protection of CUI. This encryption guideline must be followed unless an alternative physical safeguard is in place to protect CUI.

Example

You are an IT administrator responsible for employing encryption on all devices that contains CUI for your organization. You install a Secure FTP server to allow CUI to be transmitted in a compliant manner. You verify that the server is using a FIPS-validated encryption module by checking the NIST Cryptographic Module Validation Program website. You turn on the “FIPS Compliance” setting for the server during configuration since that is what is required for this product in order to use only FIPS-validated cryptography.

Mapping

- NIST SP 800-53R4: SC-8(1)
- NIST SP 800-171: 3.13.8
- CIS:
- CSF: PR.AC-2

NIST SP 800-171R2 Related Security Requirement: Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

NIST SP 800-171R2 Related Discussion: This requirement applies to internal and external networks and any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of the controls for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted. See [NIST CRYPTO].

Assessment

Assessment Objective(s): Determine if:

3.13.8[a] cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.

3.13.8[b] alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.

3.13.8[c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Cryptographic mechanisms or mechanisms supporting or implementing transmission confidentiality; organizational processes for defining and implementing alternative physical safeguards].

Testing Assessment Notes:

SC: System and Communications Protection C038:SC.3.186

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.186: Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Discussion: [DRAFT NIST SP 800-171 R2]: This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include de-allocating associated TCP/IP address or port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of user inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

CMMC Clarification: Organizations should terminate the internal and external network connections associated with communication sessions at the end of the session or after a period of inactivity by deallocating (stopping) TCP/IP addresses or ports at the operating system level, and/or deallocating assignments at the application system level. This prevents malicious actors from taking advantage of an open network session or an unattended laptop at the end of the connection. Organization's must balance user work patterns and needs against security when they determine the length of inactivity that will force a termination.

Example

You are an administrator of a server that provides remote access. You read your company's policies and see that your company has decided that network connections must be terminated after being idle for 60 minutes.

Reading the documentation for your remote access software, you learn that the configuration file for the software allows you to set an idle timeout in seconds. You edit the configuration file and set the timeout to 3600 seconds and restart the remote access software. You test the software and verify that after 60 minutes of being idle, your connection is terminated.

Mapping

- NIST SP 800-53R4: SC-10
- NIST SP 800-171: 3.13.9
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

NIST SP 800-171R2 Related Discussion: This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include de-allocating associated TCP/IP address or port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-

level network connection. Time periods of user inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Assessment

Assessment Objective(s): Determine if:

3.13.9[a] a period of inactivity to terminate network connections associated with communications sessions is defined.

3.13.9[b] network connections associated with communications sessions are terminated at the end of the sessions.

3.13.9[c] network connections associated with communications sessions are terminated after the defined period of inactivity.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing network disconnect; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting or implementing network disconnect capability].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.187: Establish and manage cryptographic keys for cryptography employed in organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters.

CMMC Clarification: The organization develops processes and technical mechanisms to protect the cryptographic key's confidentiality, authenticity and authorized use in accordance to industry standards and regulations. Key management systems provide oversight, assurance, and the capability to demonstrate the cryptographic keys are created in a secure manner and protected from loss or misuse throughout their lifecycle, e.g., active, expired, revoked. For a small number of keys, this can be accomplished with manual procedures and mechanisms. As the number of keys and cryptographic units increase, automation and tool support will be required.

Key establishment best practices are identified in NIST SP 800-56A, B and C. Key management best practices are identified in NIST SP 800-57 Parts 1, 2 and 3. Example

You are an IT administrator at your organization responsible for providing key management. You have generated a public-private key pair to exchange CUI. You require all system administrators to read the company's policy on Key Management before you allow them to install the private key on their machines. No one else in the company is allowed to know or have a copy of the private key per the policy. You provide the public key to the other parties who will be sending you CUI and test the PKI to ensure the encryption is working.

Mapping

- NIST SP 800-53R4: SC-12
- NIST SP 800-171: 3.13.10
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Establish and manage cryptographic keys for cryptography employed in organizational systems.

NIST SP 800-171R2 Related Discussion: Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters.

Assessment

Assessment Objective(s): Determine if:

3.13.10[a] cryptographic keys are established whenever cryptography is employed.

3.13.10[b] cryptographic keys are managed whenever cryptography is employed.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment and management; system security plan; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibilities for cryptographic key establishment and management].

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting or implementing cryptographic key establishment and management].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.188: Control and monitor the use of mobile code.

Discussion: [DRAFT NIST SP 800-171 R2]: Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source.

CMMC Clarification: Ensure mobile code such as Java, ActiveX, Flash is authorized to execute on the network in accordance to the organization's policy and technical configuration, and unauthorized mobile code is not. Then monitor the use of mobile code through boundary devices, audit of configurations, and implement remediation activities as needed.

Example

You are an IT administrator at the organization responsible for enforcing and monitoring the use of mobile code. The organization has established a policy that addresses the use of mobile code. You configure the baseline configuration of machines on your network to disable and deny the execution of mobile code. You implement an exception process to reactivate mobile code execution only for those users with a legitimate business need.

One user complains that a web application they need to perform their job no longer works. You meet with them and verify that the web application uses ActiveX in the browser. You submit a change for the user and get it approved by the Change Review Board for your organization. Once the change is approved, you reconfigure the user's machine to allow the running of ActiveX in the browser for this individual user. You set a reminder for yourself to check in with the user at the end of the year to verify they still need that web application.

Mapping

- NIST SP 800-53R4: SC-18
- NIST SP 800-171: 3.13.13
- CIS:
- CSF: DE.CM-5

NIST SP 800-171R2 Related Security Requirement: Control and monitor the use of mobile code.

NIST SP 800-171R2 Related Discussion: Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used

maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source.

Assessment

Assessment Objective(s): Determine if:

3.13.13[a] use of mobile code is controlled.

3.13.13[b] use of mobile code is monitored.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Organizational process for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP].

Testing Assessment Notes:

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.189: Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Discussion: [DRAFT NIST SP 800-171 R2]: VoIP has different requirements, features, functionality, availability, and service limitations when compared with the Plain Old Telephone Service (POTS) (i.e., the standard telephone service). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

CMMC Clarification: Controlling VoIP technologies starts with establishing guidelines and enforcing users' proper and appropriate usage of VoIP technologies that are described in an organization's policies. Monitoring should include the users' activity for anything other than what is permitted and authorized and detection of insecure or unauthorized use of the VoIP technology. Security concerns for VoIP include eavesdropping on calls and using ID spoofing to impersonate trusted individuals.

Example 1

The organization has established an Acceptable Use Policy for using the VoIP technology. You are an IT administrator at the organization responsible for the VoIP system. You verify that the VoIP solution is setup and configured correctly with all required security settings in compliance with the company's policies and security standards. You also verify all softphone software installed for users is kept up to date and patched to address any security issues.

Example 2

You are an IT administrator at your organization. Your organization has established a policy stating that VoIP technology may not be used without permission. You do not allow users to install VoIP applications on their devices and monitor for the unapproved use of VoIP on your network.

Mapping

- NIST SP 800-53R4: SC-19
- NIST SP 800-171: 3.13.14
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

NIST SP 800-171R2 Related Discussion: VoIP has different requirements, features, functionality, availability, and service limitations when compared with the Plain Old Telephone Service (POTS) (i.e., the standard telephone service). In contrast, other telephone services are based on high-speed, digital

communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

Assessment

Assessment Objective(s): Determine if:

3.13.14[a] use of Voice over Internet Protocol (VoIP) technologies is controlled.

3.13.14[b] use of Voice over Internet Protocol (VoIP) technologies is monitored.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; VoIP implementation guidance; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; system monitoring records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Organizational process for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP].

Testing Assessment Notes:

SC: System and Communications Protection C038:SC.3.190

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.190: Protect the authenticity of communications sessions.

Discussion: [DRAFT NIST SP 800-171 R2]: Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

CMMC Clarification: The authentication of a session refers to a user entering login credentials to identify themselves to establish communication to the system. As the communication is established a unique session id is generated to identify the user session as authenticated. Organizations need to develop and implement the necessary controls to validate the identification and protect the session id from attacks such as hijacking.

Example

You are an IT administrator at your organization. You ensure that the two-factor user authentication mechanism for the servers is setup and configured correctly. You maintain the digital certificate your company purchased and replace it with a new one before the old on expires. You ensure the TLS configuration settings on the web servers, VPN solution, and other components that use TLS are correct, using secure settings that address risks against attacks on the encrypted sessions.

Mapping

- NIST SP 800-53R4: SC-23
- NIST SP 800-171: 3.13.15
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement: Protect the authenticity of communications sessions.

NIST SP 800-171R2 Related Discussion: Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

Assessment

Assessment Objective(s): Determine if the authenticity of communications sessions is protected.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

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

Interview Assessment Notes:

Test: [SELECT FROM: Mechanisms supporting or implementing session authenticity].

Testing Assessment Notes:

SC: System and Communications Protection C038:SC.3.191

Maturity Level 3

Capability C038: Define security requirements for systems and communications

Practice SC.3.191: Protect the confidentiality of CUI at rest.

Discussion: [DRAFT NIST SP 800-17 R2]: Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest.

CMMC Clarification: CUI at rest means information that does not move through the network and may be stored on hard drives, media, and mobile devices. Develop a scheme and implement the necessary security controls to protect the confidentiality of CUI at rest. Although an approved encryption method protects data stored at rest, there are other additional technical solutions. The scheme you choose should depend on your organization's environment and business needs.

Example 1

You are an IT administrator at your organization responsible for protecting CUI at rest. Your company has a policy stating CUI must be protected at rest and you work to enforce that policy.

You research Full Disk Encryption (FDE) products that meet the FIPS encryption requirement. After testing, you roll out the encryption to all computers at your company to protect CUI at rest.

Example 2

You are an IT administrator for your company. While you have used encryption to protect the CUI on most of the computers at your company, you have some devices that do not support encryption. Your company creates a policy requiring these devices to be signed out when needed, stay in possession of the signer when checked out, and to be signed back in and locked up in a secured closet when the user is done with the device. At the end of the day each Friday, you audit the sign-out sheet and make sure all devices are returned to the closet.

Mapping

- NIST SP 800-53R4: SC-28
- NIST SP 800-171: 3.13.16
- CIS: 14.8
- CSF: PR.DS-1

NIST SP 800-171R2 Related Security Requirement: Protect the confidentiality of CUI at rest.

NIST SP 800-171R2 Related Discussion: Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The

focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. See [NIST CRYPTO].

Assessment

Assessment Objective(s): Determine if the confidentiality of CUI at rest is protected.

Assessment Objective(s) Notes:

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

Examination Assessment Notes:

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

Interview Assessment Notes:

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

Testing Assessment Notes:

Maturity Level 3

Capability C039: Control communications at system boundaries

Practice SC.3.192: Implement Domain Name System (DNS) filtering services.

Discussion: [CIS CONTROLS V7.1]: Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering. This practice is based on the following CIS control:

7.7 Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

CMMC Clarification: Domain Name System (DNS) filtering blocks access to certain websites or IP addresses. The organization should use DNS to prevent access to known malicious websites or categories of websites. The DNS filtering will prevent users from receiving an IP address for the blocked domain names. A commercial DNS filtering service can be used.

Example

You are in charge of IT operations for your company. Part of your role is to implement web browser protections. To do this, you purchase a commercial DNS filtering application or service and configure your enterprise environment to use the service. The configuration blocks users from being able to access known malicious websites. The application provider is responsible for ensuring it has the latest list of known malicious websites. As an administrator, you can update this filtering mechanism for your organization, as appropriate, to provide additional DNS blocking or to allow previously blocked websites.

Mapping

- NIST SP 800-53R4: SC-20
- NIST SP 800-171:
- CIS: 7.7
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

SC: System and Communications Protection C039:SC.3.193

Maturity Level 3

Capability C039: Control communications at system boundaries

Practice SC.3.193: Implement a policy restricting the publication of CUI on externally-owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).

Discussion: [CMMC]: Define and enforce a policy that restricts employees from publishing or posting CUI on public websites such as forums and social media outlets.

CMMC Clarification: Establish a defined and communicated policy to prohibit employees from posting CUI on a publicly facing website. This includes social media outlets such as Facebook, LinkedIn, and Twitter. This policy applies to business related and personal posts.

Example

You are a program manager for a contract that uses CUI. To ensure you are protecting your information correctly, you inform everyone working on the project of your existing policy that prohibits the posting of CUI on public websites. This includes any job- or industryrelated forums or discussions that may reference your contract work. You include these instructions in your initial project kick-off briefing and in the briefing to any employees who join the project once it is underway. You also include a reminder in your company's annual security training.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C038: Define security requirements for systems and communications

Practice SC.4.197: Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.

Discussion: [DRAFT NIST SP 800-171B]: Physical and logical isolation techniques applied at the architectural level of the system can limit the unauthorized flow of CUI; reduce the system attack surface; constrain the number of system components that must be highly secure; and impede the movement of an adversary. Physical and logical isolation techniques when implemented with managed interfaces, can isolate CUI into separate security domains where additional protections can be applied. Any communications across the managed interfaces (i.e., across security domains), constitutes remote access, even if the communications stay within the organization. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from and susceptibility to hostile cyber-attacks and errors. The degree of isolation varies depending upon the boundary protection mechanisms selected. Boundary protection mechanisms include routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; virtualization and micro-virtualization techniques; encrypting information flows among system components using distinct encryption keys; cross-domain devices separating subnetworks; and complete physical separation (i.e., air gaps).

Architectural strategies include logical isolation, partial physical and logical isolation, or complete physical isolation between subsystems and at system boundaries between resources that store, process, transmit, or protect CUI and other resources. Examples include:

- Logical isolation: data tagging, digital rights management (DRM), and data loss prevention (DLP) that tags, monitors, and restricts the flow of CUI; virtual machines or containers that separate CUI and other information on hosts; and virtual local area networks (VLAN) that keep CUI and other information separate on networks.

- Partial physical and logical isolation: physically or cryptographically isolated networks; dedicated hardware in data centers; and secure clients that: (a) may not directly access resources outside of the domain (i.e., all networked applications execute as remote virtual applications hosted in a DMZ or internal and protected enclave); (b) access via remote virtualized applications or virtual desktop with no file transfer capability other than with dual authorization; or (c) employ dedicated client hardware (e.g., a zero or thin client) or hardware approved for multi-level secure (MLS) usage.

- Complete physical isolation: dedicated (not shared) client and server hardware; physically isolated, stand-alone enclaves for clients and servers; and (a) logically separate network traffic (e.g., using a VLAN) with end-to-end encryption using PKIbased cryptography, or (b) physically isolate it from other traffic.

Isolation techniques are selected based on a risk management perspective that balances the threat, the information being protected, and the cost of the options for protection. Architectural and design decisions are guided and informed by the security requirements and selected solutions.

NIST SP 800-160-1 provides guidance on developing trustworthy secure systems using systems security engineering practices and security design concepts.

CMMC Clarification: Where the organization deems appropriate they will physically or logically isolate systems containing or processing CUI data from other systems supporting non-CUI business operations. Access controls are implemented to prevent non-authorized users from accessing the networks containing systems hosting and processing CUI information.

Example 1

You are the senior IT engineer for your organization and have been asked to install and secure a new server that will be used to store and process CUI data. You create a new VLAN and directly connect the server to that VLAN. Then you configure an Access Control List (ACL) to block that VLAN from getting out to the Internet and only allows the analysts working on the program to have access to that server.

Example 2

You are managing a project working on CUI data with two other people. You identify a room and provide only the team members and yourself with keys to access the room. You have the server and a small workgroup switch installed in the room with a couple of workstations. The workgroup switch is not connected to the organization's network so team members must go to work in the locked room to work on this project.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 14.1
- CSF: PR.AC-5

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C038: Define security requirements for systems and communications

Practice SC.4.228: Isolate administration of organizationally defined high-value critical network infrastructure components and servers.

Discussion: [CMMC]: Organizations apply systems security engineering concepts and principles to identify the high value critical network infrastructure components in their network. High value critical systems are those that if compromised could lead to unauthorized access, use, modification or destruction of large amounts of CUI. Examples include boundary protection systems (e.g., routers, firewalls, intrusion protection and detection systems), critical infrastructure servers (e.g., domain, policy, certificate) and key servers processing CUI (e.g., file, mail, collaboration applications) Securing administration, the ability to alter the configuration of these components, includes delineating physical and logical security boundaries between the data and management interfaces such as through the use of an Out-of-Band network.

NIST Special Publication 800-160 provides guidance on systems security engineering.

CMMC Clarification: Where the organization has identified high value critical network infrastructure used in the processing and management of CUI data, they will physically or logically isolate management these systems from their production network, such as through the use of an Out-of-Band network. Access controls are implemented to prevent non-authorized users from accessing the management network and changing the configuration of an infrastructure component processing CUI information.

Example 1

You are responsible for security architecture and are asked to build and secure a network enclave to support a large project processing CUI data from two facilities in your organization. The architecture you designed to support this project has a workgroup switch in each location connected to a firewall to the Internet. The management interfaces on the two switches and the firewall are all connected to the Out-of-Band (OOB) management network that is air-gapped from the rest of the company and the Internet.

Example 2

You have created VLANs that are used to access the management interface of all the network switches and the servers in the data center. These VLANs are isolated from the rest of the organization's network so only the network engineers and server administrators can manage these devices from their offices or a Bastion Host server you set up.

Mapping

- NIST SP 800-53R4: SA-8
- NIST SP 800-171: 3.13.2
- CIS: 11.7,14.1
- CSF: PR.AC-5

NIST SP 800-171R2 Related Security Requirement: Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

NIST SP 800-171R2 Related Discussion: Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

Assessment

Assessment Objective(s): Determine if:

3.13.2[a] architectural designs that promote effective information security are identified.

3.13.2[b] software development techniques that promote effective information security are identified.

3.13.2[c] systems engineering principles that promote effective information security are identified.

3.13.2[d] identified architectural designs that promote effective information security are employed.

3.13.2[e] identified software development techniques that promote effective information security are employed.

3.13.2[f] identified systems engineering principles that promote effective information security are employed.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; system and communications protection policy; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; security architecture documentation; security requirements and specifications for the system; system design documentation; system configuration settings and associated documentation; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with responsibility for determining information system

Interview Assessment Notes:

Test: [SELECT FROM: Separation of user functionality from system management functionality].

Testing Assessment Notes:

Maturity Level 4

Capability C039: Control communications at system boundaries

Practice SC.4.199: Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.

Discussion: [CMMC]: Threat intelligence can provide information on known, bad domain names. Using that information to prevent access by blocking DNS requests for those domains is one way to prevent an organization from being attacked with watering hole attacks or malicious downloads.

CMMC Clarification: As part of collecting threat intelligence from a variety of sources such as government, industry peer organizations, or commercial services, use the known, bad domain names to feed security mechanisms (e.g., DNS servers or firewalls). Implement checks in the organization's system to ensure devices making DNS calls to malicious sites are blocked from getting to those sites. This practice explicitly requires the use of threat intelligence in its application. This differs from the DNS filtering in practice SC.3.192 that allows for other means of creating the filters.

Example

You are responsible for network security for your organization and participate in the National Defense Information Sharing and Analysis Center (ND-ISAC) working groups. You subscribe to automated feeds from ND-ISAC and electronic sharing with your peers to learn about new malware sites and update your DNS server to black hole access to them.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C039: Control communications at system boundaries

Practice SC.4.202: Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.

Discussion: [CMMC]: Advanced malicious executable code has become much better at evading signature-based detection and protection capabilities. Sandboxes and other advanced analytics are more advanced defenses that allow the code or script to execute in an isolated, controlled, and instrumented environment to detect signs of malicious activity.

CMMC Clarification: The organization shall install systems that automatically analyze executable and mobile code passing through the system boundary (e.g., downloaded from the Internet or other transmission method.) This practice is not focused on email, which is covered in practice SI.3.220. Any executable or mobile code identified as suspicious should be quarantined and not allowed to pass through to the user until confirmed not to be malware or required for a business purposes.

Example

You are the data security manager for the organization. You have learned that staff routinely browse the Internet and download PDF files and executables as part of their work assignments. To ensure the downloaded files do not contain malware, you install a sandbox appliance in the DMZ which checks all downloads for malicious content.

Mapping

- NIST SP 800-53R4: SC-44
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

SC: System and Communications Protection C039:SC.4.229

Maturity Level 4

Capability C039: Control communications at system boundaries

Practice SC.4.229: Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.

Discussion: [CMMC]: Typically a high percentage of an organization's internet traffic is web-based. Web-based information and services is access through a Uniform Resource Locator (URL). Information regarding the provenance and purpose of a URL can be used to restrict access for policy or security concerns.

CMMC Clarification: Organizations shall have the ability to prevent access to URLs the organization has determined should not be accessed for policy or security reasons. URL filters typically are a blacklist of URLs that block access to known bad sites. Categorization services identify websites according to a set of content attributes and allow organizations to allow or disallow access to entire classes of websites. In addition, organizations may choose to block access to uncategorized sites, which may represent malicious sites. The filters and categories should be updated dynamically through an intel subscription as well as manually.

Example 1

You are the security manager for the organization. You installed a web proxy and configured all the computers in the organization to use the proxy to access HTTP and HTTPS sites on the Internet. The proxy servers are updated daily with the vendor's URL categorization database and you put in rules to block access to hate, gambling, and porn sites as well as all sites that have not yet been categorized.

Example 2

You are the IT manager for the organization. You evaluated and selected a cloud filtering service that allowed you to create and manage policies for which sites users could access. To start using the service, you redirect the organization's DNS to point to the cloud provider so everyone in the organization would be covered by the URL access policies you established.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 7.4
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C038: Define security requirements for systems and communications

Practice SC.5.198: Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizational-defined boundaries.

Discussion: [CIS CONTROLS V7.1]: Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

CMMC Clarification: The organization shall capture and save all packets traversing the network boundary for a period of time determined by the organization. The system will support detailed analysis of an event showing what packets were transmitted and received and be able to reconstruct and determine content transmitted during a specific time period.

Example

You manage security systems for the organization. You purchase a network recorder appliance and install it between the firewall and the Internet router to record all traffic entering or exiting the organization's network. The network recorder is configured to retain three months of network traffic.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS: 12.5
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

SC: System and Communications Protection C038:SC.5.230

Maturity Level 5

Capability C038: Define security requirements for systems and communications

Practice SC.5.230: Enforce port and protocol compliance.

Discussion: [CMMC]: Malicious actors are able to perform command and control and exfiltration of data by running their own protocols over well-known ports or by hijacking fields within a common protocol. By defining allowed ports and protocols, and only allowing proper protocol syntax on the correct authorized ports, the malicious activity is stopped.

CMMC Clarification: Organizations shall enforce traffic crossing the network boundary is in compliance with the standard for the protocol in question and using the appropriate well-known port. If the port or protocol is not known the traffic should be blocked.

Example 1

You are a network engineer for your organization. You have a NextGen firewall installed on the Internet edge of the network and have configured the firewall to perform protocol enforcement and block traffic that is not known or specifically approved by the organization's security policy.

Example 2

You are a network engineer for your organization. You have configured the IPS device to monitor and block traffic that is not in compliance with standard or protocols approved for users to access the Internet.

Mapping

- NIST SP 800-53R4: AC-7(17)
- NIST SP 800-171:
- CIS: 9.2
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C039: Control communications at system boundaries

Practice SC.5.208: Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.

Discussion: [CMMC]: Advanced adversaries study and analyze standard commercial security solutions and standard configurations of those systems. They develop and test attack techniques that will not be mitigated by those solutions. Tailoring protections forces the adversary to confront a security solution or configuration that they have not seen anywhere else. They will not have developed a way around it.

CMMC Clarification: Organizations shall tailor the configuration and function of one or more of their boundary protection systems so it will mitigate (protect or detect) attack activities in some manner not typical of commercial security solutions. This can range from an internally developed security solution to just custom configurations and signatures.

Example 1

You manage the organization's Intrusion Prevention System (IPS) system. You analyzed several phishing emails containing malware scripts and noticed similarities between them. You create a custom rule in the IPS to monitor for and block emails that matched this signature.

Example 2

You are the network security manager for the company. You are responsible for checking the vendor signatures on the IPS and checking that sandboxing appliances are being updated automatically. You write custom rules to alert on zero-day vulnerabilities the ND-ISAC has reported.

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 1

Capability C040: Identify and manage information system flaws

Practice SI.1.210: Identify, report, and correct information system flaws in a timely manner.

Discussion: [DRAFT NIST SP 800-171 R2]: Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation. NIST SP 800-40 provides guidance on patch management technologies.

CMMC Clarification: All software and firmware have potential flaws. Many vendors work to reduce those flaws by releasing vulnerability information and updates to their software and firmware. Organizations should have a process to review relevant vendor newsletters with updates about common problems or weaknesses. After reviewing the information the organization should execute a process called patch management that allows for systems to be updated without adversely affecting the organization. Organizations should also purchase support from their vendors to ensure timely access to updates.

Example

You have many responsibilities at your company, including IT. You know that malware, ransomware, and viruses can be a big problem for companies. You make sure to enable all security updates for your software, including the operating system and applications, and purchase the maintenance packages for new hardware and operating systems.

Mapping

- NIST SP 800-53R4: SI-2
- NIST SP 800-171: 3.14.1
- CIS:
- CSF: RS.CO-2,RS.MI-3

NIST SP 800-171R2 Related Security Requirement: Identify, report, and correct system flaws in a timely manner.

NIST SP 800-171R2 Related Discussion: 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.

Assessment

Assessment Objective(s): Determine if:

3.14.1[a] the time within which to identify system flaws is specified.

3.14.1[b] system flaws are identified within the specified time frame.

3.14.1[c] the time within which to report system flaws is specified.

3.14.1[d] system flaws are reported within the specified time frame.

3.14.1[e] the time within which to correct system flaws is specified.

3.14.1[f] system flaws are corrected within the specified time frame.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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 managemen

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting or implementing reporting, and correcting system flaws; mechanisms s

Testing Assessment Notes:

Maturity Level 1

Capability C041: Identify malicious content

Practice SI.1.211: Provide protection from malicious code at appropriate locations within organizational information systems.

Discussion: [DRAFT NIST SP 800-171 R2]: Designated locations include system entry and exit points which may include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. NIST SP 800-83 provides guidance on malware incident prevention.

CMMC Clarification: You can protect your company's valuable IT system by stopping malicious code at designated locations in your system. Malicious code is program code that purposefully creates an unauthorized function or process that will have a negative impact on the confidentiality, integrity, or availability of an information system. A designated location may be your network device or your computer.

Malicious code includes the following, which can be hidden in email, email attachments, web access:

- viruses, programs designed to damage, steal information, change data, send email, show messages, or any combination of these things;
- spyware, a program designed to gather information about a person's activity in secret, and is usually installed without the person knowing when they click on a link; and
- a trojan horse, a type of malware made to look like legitimate/real software, and used by cyber criminals to get access to a company's systems.

By using anti-malware tools, you can stop or lessen the impact of malicious code.

Example

You are buying a new computer for your small business and want to protect your company's information from viruses, spyware, etc. You buy and install anti-malware software.

Mapping

- NIST SP 800-53R4: SI-3
- NIST SP 800-171: 3.14.2
- CIS: 8.1
- CSF: DE.CM-4

NIST SP 800-171R2 Related Security Requirement: Provide protection from malicious code at designated locations within organizational systems.

NIST SP 800-171R2 Related Discussion: Designated locations include system entry and exit points which may include firewalls, remoteaccess servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputationbased 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.

Assessment

Assessment Objective(s): Determine if:

3.14.2[a] designated locations for malicious code protection are identified.

3.14.2[b] protection from malicious code at designated locations is provided.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

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, up

Testing Assessment Notes:

Maturity Level 1

Capability C041: Identify malicious content

Practice SI.1.212: Update malicious code protection mechanisms when new releases are available.

Discussion: [DRAFT NIST SP 800-171 R2]: Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other.

CMMC Clarification: You can protect your company's valuable IT systems by staying up to date on new security releases that stop malicious code and monitoring the system regularly. Malicious code is program code that is always changing, so it is important to always have up-to-date protections, such as anti-malware tools.

Example

You bought a new computer for your small business. You know that you need to protect your company's information from viruses, spyware, etc. So, you also purchased and installed antimalware software. You configure the software to automatically update to the latest antivirus code and definitions of all known malware.

Mapping

- NIST SP 800-53R4: SI-3
- NIST SP 800-171: 3.14.4
- CIS: 8.2
- CSF: DE.CM-4

NIST SP 800-171R2 Related Security Requirement: Update malicious code protection mechanisms when new releases are available.

NIST SP 800-171R2 Related Discussion: Malicious code protection mechanisms include anti-virus signature definitions and reputationbased 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.

Assessment

Assessment Objective(s): Determine if malicious code protection mechanisms are updated when new releases are available.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

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 cod

Testing Assessment Notes:

SI: System and Information Integrity C041:SI.1.213

Maturity Level 1

Capability C041: Identify malicious content

Practice SI.1.213: Perform periodic scans of information systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Discussion: [DRAFT NIST SP 800-171 R2]: Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. Many technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyberattacks 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.

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

Example

While cleaning up your office, you find your old thumb drive. You are not sure if you should use it. Then you remember something: Your company just purchased anti-malware software that auto-updates with the latest antivirus code and definitions of all known malware. With this in mind, you decide to plug in the thumb drive. The new anti-malware software scans the thumb drive, finds a virus, then deletes the file.

Mapping

- NIST SP 800-53R4: SI-3
- NIST SP 800-171: 3.14.5
- CIS: 8.4,8.7
- CSF: DE.CM-4

NIST SP 800-171R2 Related Security Requirement: Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

NIST SP 800-171R2 Related Discussion: Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Assessment

Assessment Objective(s): Determine if:

3.14.5[a] the frequency for malicious code scans is defined.

3.14.5[b] malicious code scans are performed with the defined frequency.

3.14.5[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

Assessment Objective(s) Notes:

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].

Examination Assessment Notes:

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

Interview Assessment Notes:

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 cod

Testing Assessment Notes:

Maturity Level 2

Capability C040: Identify and manage information system flaws

Practice SI.2.214: Monitor system security alerts and advisories and take action in response.

Discussion: [DRAFT NIST SP 800-171 R2]: There are many publicly available sources of system security alerts and advisories. The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and relevant industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations.

NIST SP 800-161 provides guidance on supply chain risk management.

CMMC Clarification: Organizations should receive security alerts, advisories, and directives from reputable external organizations. You base identification of these organizations on sector, industry, and the technology you use. There are many ways to received alerts and advisories and may include:

- signing up for email distributions;
- subscribing to RSS feeds; and
- attending meetings.

Organizations should review alerts and advisories for applicability as they receive them. An organization decides on its own review cycle. The more frequent the alerts and advisories, the more frequent the reviews. This ensures that the organization has the most up-to-date information.

External alerts and advisories may prompt an organization to generate internal security alerts, advisories, or directives. Share these with all personnel with a need-to-know. The individuals should take action to respond to the alerts. Actions vary according to the alert or advisory. Sometimes it may require a system configuration update. Other times, the organization may use the information for situational awareness purposes.

Example

One of your IT responsibilities is to protect your organization’s computers. As part of your job you decide you need to pay attention to security alerts and advisories to keep aware of the latest threats and risks. You decide to receive alerts from US-CERT and a set of ISACs. You review the alerts on a weekly basis to determine if they are relevant to your organization. When you identify one you follow your plan to correct information system flaws in a timely manner, such as installing a patch.

Mapping

- NIST SP 800-53R4: SI-5
- NIST SP 800-171: 3.14.3

- CIS: 6.5,6.6
- CSF: RS.AN-5

NIST SP 800-171R2 Related Security Requirement: Monitor system security alerts and advisories and take action in response.

NIST SP 800-171R2 Related Discussion: There are many publicly available sources of system security alerts and advisories. For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations

Assessment

Assessment Objective(s): Determine if:

3.14.3[a] response actions to system security alerts and advisories are identified.

3.14.3[b] system security alerts and advisories are monitored.

3.14.3[c] actions in response to system security alerts and advisories are taken.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and information integrity policy; procedures addressing security alerts, advisories, and directives; system security plan; records of security alerts and advisories; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: Personnel with security alert and advisory responsibilities; personnel implementing, operating, maintaining, and using the system; personnel, organizational elements, and external organizations to whom alerts, advisories, and directives are

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; mechanisms supporting or implementing definition, receipt, generation, and dissemination of security

Testing Assessment Notes:

Maturity Level 2

Capability C042: Perform network and system monitoring

Practice SI.2.216: Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Discussion: [DRAFT NIST SP 800-171 R2]: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

NIST SP 800-94 provides guidance on intrusion detection and prevention systems.

CMMC Clarification: Organizations should leverage their monitoring systems to look for indicators of attacks. Think of indicators of attack as a series of actions that an adversary conducts in advance of an attack. Indicators of attack concern the steps involved and the intent of the adversary.

Indicators of attacks on organizational systems may include:

- internal traffic that indicates the presence of malicious code;
- malicious code detected during non-business hours;
- the unauthorized data leaving the organization; and

- communicating to external information systems.

To detect attacks and indicators of attacks with success, deploy monitoring devices. Place these devices within the systems at strategic points to collect essential information. Strategic points include internal and external system boundaries. The organization should monitor both inbound traffic and outbound traffic.

Example

You are in charge of IT operations at your organization. You look for attacks to your network. To do this, you monitor all organizational systems. You also watch communications to and from your machines. You look for indicators, or things that don't look like they should. These indicators can show up in many places on your network. You should monitor important places on your network. These places might include:

- perimeter locations, or locations your networks connect to the internet;
- machines that have important software or data on them that attackers might want to access; and
- your remote connections which may be a way to gain access to your network from the outside.

Perform additional monitoring when you find an indicator, or something that doesn't perform as it should. This extra monitoring should tell you if it is a current or potential attack.

Set up your monitoring activities so that they support your organization's planning. Develop your monitoring requirements as part of your organization's security activities. Ensure that your monitoring activities meet the security needs of your organization.

Mapping

- NIST SP 800-53R4: SI-4
- NIST SP 800-171: 3.14.6
- CIS: 12.6
- CSF: DE.CM-1

NIST SP 800-171R2 Related Security Requirement: Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

NIST SP 800-171R2 Related Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

Assessment

Assessment Objective(s): Determine if:

3.14.6[a] the system is monitored to detect attacks and indicators of potential attacks.

3.14.6[b] inbound communications traffic is monitored to detect attacks and indicators of potential attacks.

3.14.6[c] outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: System and information integrity policy; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram or layout; system security plan; system monitoring tools and techniques documentation; system design documentation; locations within system where monitoring devices are deployed; system protocols; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility monitoring the system; personnel with responsibility for the

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing intrusion detection capability and system monitoring; mechanisms supporting or implementing system monitoring capability; organizational processes for intr

Testing Assessment Notes:

Maturity Level 2

Capability C042: Perform network and system monitoring

Practice SI.2.217: Identify unauthorized use of organizational systems.

Discussion: [DRAFT NIST SP 800-171 R2]: System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs.

Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

NIST SP 800-94 provides guidance on intrusion detection and prevention systems.

CMMC Clarification: Organizations should define authorized use of their systems. First, have an acceptable-use policy for your system. This policy establishes the baseline for how users access devices and the internet. You define authorized use by specific roles within the organization. Examples of these roles include user, administrator, and technician. After you define authorized use, identify unauthorized use of systems.

Organizations can monitor systems by observing audit activities. You can do this in real time or by other manual means, such as access patterns. To identify unauthorized use, leverage existing tools and techniques, such as:

- intrusion detection systems;
- intrusion prevention systems;
- malicious code protection software;
- scanning tools;
- audit record monitoring software; and
- network monitoring software.

Example

You are in charge of IT operations at your organization. You want to make sure everyone using an organizational system is authorized to do so. You accomplish this as part of your monitoring activities. These activities ensure that all users meet the defined authorize-use policy. To do this, you put in place a

user activity monitoring application. This app monitors all the users and their connections to your network. It records information about every connection on your network. You use the outputs of this application to confirm that you are meeting the authorization policy.

Mapping

- NIST SP 800-53R4: SI-4
- NIST SP 800-171: 3.14.7
- CIS:
- CSF: DE.CM-1,DE.CM-7

NIST SP 800-171R2 Related Security Requirement: Identify unauthorized use of organizational systems.

NIST SP 800-171R2 Related Discussion: System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs.

Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

Assessment

Assessment Objective(s): Determine if:

3.14.7[a] authorized use of the system is defined.

3.14.7[b] unauthorized use of the system is identified.

Assessment Objective(s) Notes:

Examine: [SELECT FROM: Continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram/layout; system security plan; system design documentation; system monitoring tools and techniques documentation; locations within system where monitoring devices are deployed; system configuration settings and associated documentation; other relevant documents or records].

Examination Assessment Notes:

Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for monitoring the system].

Interview Assessment Notes:

Test: [SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing system monitoring capability].

Testing Assessment Notes:

Maturity Level 3

Capability C042: Perform network and system monitoring

Practice SI.3.218: Employ spam protection mechanisms at information system access entry and exit points.

Discussion: [CMMC]: Spam filtering is used to protect against unwanted, unsolicited, and often harmful emails from reaching end user mailboxes. Spam filters are applied on inbound and outbound emails. Spam filtering helps protect your network from phishing and emails containing viruses and other malicious content. Spam filtering can also be used to mark email as potential spam to caution users reading the email and clicking on links within the email. Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers.

CMMC Clarification: Spam filters should be applied on email that is inbound (coming into the organization) or outbound (leaving the organization). Inbound filters can protect the organization's users from spam originating on the internet. Outbound protection helps the organization identify the origins of potential spam on their own network. Without this, an organization risks having its email server blacklisted for sending spam emails.

Example

As the email administrator for your company, you notice a significant increase in the amount of spam entering your network year after year. You want to implement a spam filtering capability to meet these two goals:

- reduce the number of unsolicited email to your user's inboxes; and
- block potentially harmful email, including phishing emails and attachments, from reaching end users.

You create a spam mailbox where users can forward spam emails that make it through the filter. You periodically review the spam mailbox emails and use them to improve the spam filter rules to better block spam in the future.

You are also concerned that, without adding outbound spam protections, your organization's email servers could be blacklisted. Because of this, you implement outbound protections that allow you to trace potential spam email originating on your network to a specific user and machine.

Mapping

- NIST SP 800-53R4: SI-8
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

SI: System and Information Integrity C043:SI.3.219

Maturity Level 3

Capability C043: Implement advanced email protections

Practice SI.3.219: Implement email forgery protections.

Discussion: [CMMC]: Protecting your environment from harmful emails is one of the best ways to reduce the risk of viruses and malware from entering your network. Email attacks are one of the primary attack vectors in use by threat actors today because of their simplicity and effectiveness for circumventing an organization's perimeter defenses. Implementing advanced email protections can help mitigate these email-based threats from penetrating an organization's defenses and landing in the inbox of organizational end users.

CMMC Clarification: Implement email protections in addition to basic spam protections. Some potential advanced email protections include Sender Policy Framework (SPF) ,Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance

(DMARC). SPF uses DNS to show which servers are allowed to send email for a given domain. DKIM uses asymmetric cryptography to verify the authenticity of an email message and provide assurance of the legitimacy of the email to the recipient. DMARC allows organizations to deploy a combination of DKIM and SPF to further enhance their electronic mail infrastructure by adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

Example

As the email administrator for your organization, you want to add additional protections to ensure you are blocking as many unwanted and harmful emails as possible. You configure a DMARC policy that enables both SPF and DKIM on your domain. You configure an SPF text entry in your DNS configuration so that you explicitly authorize the servers that can send email as well as ensuring relevant outbound emails are signed using DKIM.

Mapping

- NIST SP 800-53R4: SC-8
- NIST SP 800-171:
- CIS: 7.8
- CSF: PR.DS-2

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

SI: System and Information Integrity C043:SI.3.220

Maturity Level 3

Capability C043: Implement advanced email protections

Practice SI.3.220: Utilize sandboxing to detect or block potentially malicious email.

Discussion: [CIS CONTROLS V7.1]: Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering. This practice is based on the following CIS control:

7.10 Use sandboxing to analyze and block inbound email attachments with malicious behavior.

CMMC Clarification: You create an email sandbox by implementing an isolated environment to execute an attached file or linked URL. Before allowing attachments or links to be opened on the production network, they are executed within the sandbox and their behavior is observed. By opening these files or links in a protected environment, the system detects malicious activity before it is introduced into the network.

Example

You are in charge of IT operations for your organization. Part of your role is to verify all attachments and URL links in company emails. To do this, you set-up an isolated environment, or email sandbox, to execute or open all email attachments before allowing them on your network. You use the email sandbox to observe what happens when the attachment or link opens. By testing these files in a sandbox, you are able to prevent the entry of malicious content through email attachments or URL links. You only allow emails with attachments or URL links through once they have been tested and determined to be safe.

Mapping

- NIST SP 800-53R4: SC-44
- NIST SP 800-171:
- CIS: 7.1
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 4

Capability C040: Identify and manage information system flaws

Practice SI.4.221: Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.

Discussion: [DRAFT NIST SP 800-171B]: The constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), make it essential that threat information relating to specific threat events (e.g., TTP, targets) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur) be sourced from and shared with trusted organizations. This information can be used by organizational Security Operations Centers (SOC) and incorporated into monitoring capabilities. Threat information sharing includes threat indicators, signatures, and adversary TTP from organizations participating in various threat-sharing consortia, government-commercial cooperatives, and government-government cooperatives (e.g., CERTCC, US-CERT, FIRST, ISAO, DIB CS Program). Unclassified indicators, based on classified information but which can be readily incorporated into organizational intrusion detection systems, are available to qualified nonfederal organizations from government sources.

CMMC Clarification: When conducting cyberattacks the attackers tend to operate using certain patterns of behavior or exploit capabilities. This collection of patterns and capabilities are known as Tactics, Techniques, and Procedures (TTP). An organization can build their knowledge of attacker TTPs by participating in Information Sharing and Analysis Centers (ISAC) for their industry. An ISAC collects cyber threat information relevant to the industry and its members in order to improve the cyber posture of that industry. Based on the lines of business an organization may consider more than one ISAC. An organization may also acquire TTPs through commercial providers in order to integrate into various technologies.

Example

You are the manager of the Security Operations Center (SOC) and have recently added a role to perform cyber threat hunting. You have been tasked to set up the process for the SOC. You first identify relevant sources of threat information for the organization. You have the organization join the National Defense ISAC and begin to interact with peers in the ISAC. You capture events in your organization and share the TTPs with your peers. In return, they share new TTPs with you. After downloading the TTPs, you build queries against the SOC's central repository for recurring searches. You also acquire a commercial threat indicator feed of suspicious domains, known malware hashes, and IP addresses. You use these to supplement a custom intrusion detection system.

ADDITIONAL READING

National Council of ISACs: https://www.nationalisacs.org/

ATT&CK: https://attack.mitre.org/

NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Homeland Security Systems Engineering & Development Institute Cyber Threat Modeling: https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threatmodeling.pdf

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF: ID.RA-2,ID.RA-3

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C041: Identify malicious content

Practice SI.5.222: Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.

Discussion: [CMMC]: Organizations deploy preventive measures such as anti-virus or application whitelisting to reduce the effects of malware executables on endpoints. As the use of whitelisting becomes a more pervasive defense technique attackers are leveraging trusted operating systems software, scripts, or code to perform malicious activities including lateral movement and persistence. By using these tactics, the attacker seeks to reduce the chances of being discovered. This move to "living off the land" needs to be mitigated by analyzing the use and behavior of system commands and utilities.

CMMC Clarification: Normal system commands and scripts used by the adversary will be allowed by normal application whitelists. The adversary uses this fact to move around despite the presence of whitelisting or other defenses. An organization may use endpoint detection and response (EDR) to record system activities and events that occur. Analyzing EDR records is one way to identify execution of a script that operates outside of normal parameters, indicating an exploit is in progress. Another way to approach this is to use User and Entity Behavior Analytics solutions to identify malicious activity.

Example

As part of your cyber defenses the organization has deployed EDR to laptops and desktops. Recent threat intelligence indicates an increased use of Powershell attacks. Powershell provides a shell and script language to Window's system functions. Its versatility makes it useful for system admininstrators as well as adversaries. Adversaries no longer need to download their own utilities which could be identified by common anti-malware software. Since you know the adversary will try to move around your network you focus on identifying lateral movement. You tune your EDR software to monitor for scripts run on remote computers and interactive remote shell sessions across your organizations's laptops and desktops.

ADDITIONAL READING

Symantec Living off the land and fileless attack techniques:

https://www.symantec.com/content/dam/symantec/docs/security-center/whitepapers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops: https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final

Mapping

- NIST SP 800-53R4:
- NIST SP 800-171:
- CIS:
- CSF:

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes:

Maturity Level 5

Capability C042: Perform network and system monitoring

Practice SI.5.223: Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.

Discussion: [DRAFT NIST SP 800-171B]: Monitoring is used to identify unusual or unauthorized activities or conditions related to individual users and system components, for example, unusual internal systems communications traffic; unauthorized exporting of information; signaling to external systems; large file transfers; long-time persistent connections; attempts to access information from unexpected locations; unusual protocols and ports in use; and attempted communications with suspected malicious external addresses

The correlation of physical audit record information and the audit records from systems may assist organizations in identifying examples of anomalous behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional information that the individual was not present at the facility when the logical access occurred, is indicative of anomalous behavior. Indications of increased risk from individuals can be obtained from many sources including human resource records, intelligence agencies, law enforcement organizations, and other sources. The monitoring of specific individuals is closely coordinated with management, legal, security, privacy, and human resource officials in organizations conducting such monitoring, and in certain circumstances requires the prior authorization by a specified senior organizational official.

CMMC Clarification: Monitoring for anomalous or suspicious behavior can be done with signatures, statistical analysis, analytics or machine learning on user activity events. The analysis seeks to find patterns amongst data generated by user activity. This is different than traditional security applications that analyze events. This class of analysis is typically called User and Entity Behavior Analytics (UEBA).

Example

You are working the night shift in the Security Operations Center (SOC). You notice alerts related to someone from accounting. That person doesn't use their computer at this time of night so the monitoring system has identified anomalous activity. The algorithms identify activity outside business hours and an excessive data upload from a key server on the network using that account. You initiate an investigation to determine the source and risk from the data exfiltration.

ADDITIONAL READING

Ten Strategies of a World-class Cybersecurity Operations Center: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategiescyber-ops-center.pdf

SANS Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey: https://www.sans.org/media/analyst-program/common-practices-securityoperations-centers-results-2019-soc-survey-39060.pdf

Mapping

- NIST SP 800-53R4: SI-4
- NIST SP 800-171:
- CIS: 13.3,16.12,16.13
- CSF: DE.CM-1,DE.CM-3

NIST SP 800-171R2 Related Security Requirement:

NIST SP 800-171R2 Related Discussion:

Assessment

Assessment Objective(s):

Assessment Objective(s) Notes:

Examine:

Examination Assessment Notes:

Interview:

Interview Assessment Notes:

Test:

Testing Assessment Notes: