NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

National Institute of
Standards and Technology
U.S. Department of Commerce

CHAPTER THREE

THE REQUIREMENTS

SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

This chapter describes fourteen families of security requirements (including basic and derived requirements) for protecting the confidentiality of CUI in nonfederal systems and organizations.[18] The security controls from NIST Special Publication 800-53 associated with the basic and derived requirements are also listed in Appendix D.[19] Organizations can use Special Publication 800-53 to obtain additional, non-prescriptive information related to the security requirements (e.g., supplemental guidance related to each of the referenced security controls, mapping tables to ISO/IEC security controls, and a catalog of optional controls that can be used to help specify additional security requirements if needed). This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.[20]

Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should 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.

THE MEANING OF ORGANIZATIONAL SYSTEMS

The term *organizational system* is used in many of the CUI security requirements in NIST Special Publication 800-171. This term has a specific meaning regarding the scope of applicability for the CUI security requirements. The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. The appropriate scoping for the security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

[18] While the purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives. Thus, the integrity requirements (either basic or derived) may have a significant, albeit indirect, effect on the ability of an organization to protect the confidentiality of CUI.

[19] The security control references in Appendix D are included to promote a better understanding of the security requirements. The control references are not intended to impose additional requirements on nonfederal organizations. Moreover, because the security controls were developed for federal agencies, the supplemental guidance associated with those controls may not be applicable to nonfederal organizations.

[20] To promote consistency, transparency, and comparability, compensatory security measures selected by organizations should be based on or derived from *existing* and *recognized* security standards and control sets, including, for example: ISO/IEC 27001 or NIST Special Publication 800-53.

When requested, the system security plan and any associated plans of action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. 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.

The security requirements in this publication should be applied to the nonfederal organization's internal systems processing, storing, or transmitting CUI. Some systems, including specialized systems (e.g., industrial/process control systems, Computer Numerical Control machines, medical devices), may have restrictions or limitations on the application of certain security requirements. To accommodate such issues, the system security plan, as reflected in Requirement 3.12.4, should be used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies should be managed though plans of action, as reflected in Requirement 3.12.2.

Appendix F provides expanded information on the CUI security requirements. Hyperlinks in the CUI requirements below provide direct accessibility to the discussion section in the appendix.

3.1 ACCESS CONTROL

Basic Security Requirements

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

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

Derived Security Requirements

3.1.3 Control the flow of CUI in accordance with approved authorizations.

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

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

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

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

3.1.8 Limit unsuccessful logon attempts.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

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

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

3.1.12 Monitor and control remote access sessions.

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

3.1.14 Route remote access via managed access control points.

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

3.1.16 Authorize wireless access prior to allowing such connections.

3.1.17 Protect wireless access using authentication and encryption.

3.1.18 Control connection of mobile devices.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.[21]

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

3.1.21 Limit use of portable storage devices on external systems.

3.1.22 Control CUI posted or processed on publicly accessible systems.

Mapping access control requirements to controls

3.2 AWARENESS AND TRAINING

Basic Security Requirements

3.2.1 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.

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

Derived Security Requirements

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

Mapping awareness and training requirements to controls

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements

3.3.1 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.

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

Derived Security Requirements

3.3.3 Review and update logged events.

3.3.4 Alert in the event of an audit logging process failure.

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

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

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

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

[21] Mobile devices and mobile computing platforms include, for example, smartphones, tablets, E-readers, and notebook computers.

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

Mapping audit and accountability requirements to controls

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

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

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

Derived Security Requirements

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

3.4.4 Analyze the security impact of changes prior to implementation.

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

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

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

3.4.8 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.

3.4.9 Control and monitor user-installed software.

Mapping configuration management requirements to controls

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements

3.5.1 Identify system users, processes acting on behalf of users, and devices.

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

Derived Security Requirements

3.5.3 Use multifactor authentication[22] for local and network access[23] to privileged accounts and for network access to non-privileged accounts.

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

[22] *Multifactor authentication* requires two or more different factors to achieve authentication. The factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

[23] *Local access* is any access to a system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. *Network access* is any access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

3.5.5 Prevent reuse of identifiers for a defined period.

3.5.6 Disable identifiers after a defined period of inactivity.

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

3.5.8 Prohibit password reuse for a specified number of generations.

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

3.5.10 Store and transmit only cryptographically-protected passwords.

3.5.11 Obscure feedback of authentication information.

Mapping identification and authentication requirements to controls

3.6 INCIDENT RESPONSE

Basic Security Requirements

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

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Derived Security Requirements

3.6.3 Test the organizational incident response capability.

Mapping incident response requirements to controls

3.7 MAINTENANCE

Basic Security Requirements

3.7.1 Perform maintenance on organizational systems.[24]

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Derived Security Requirements

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

Mapping maintenance requirements to controls

[24] In general, system maintenance requirements tend to support the security objective of *availability*. However, improper system maintenance or a failure to perform maintenance can result in the unauthorized disclosure of CUI, thus compromising *confidentiality* of that information.

3.8 MEDIA PROTECTION

Basic Security Requirements

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

3.8.2 Limit access to CUI on system media to authorized users.

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Derived Security Requirements

3.8.4 Mark media with necessary CUI markings and distribution limitations.[25]

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.7 Control the use of removable media on system components.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

Mapping media protection requirements to controls

3.9 PERSONNEL SECURITY

Basic Security Requirements

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Derived Security Requirements

None.

Mapping personnel security requirements to controls

3.10 PHYSICAL PROTECTION

Basic Security Requirements

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

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

Derived Security Requirements

3.10.3 Escort visitors and monitor visitor activity.

3.10.4 Maintain audit logs of physical access.

3.10.5 Control and manage physical access devices.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

Mapping physical protection requirements to controls

[25] The implementation of this requirement is per marking guidance in the 32 CFR, Part 2002, and the CUI Registry.

3.11 RISK ASSESSMENT

Basic Security Requirements

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Derived Security Requirements

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

Mapping risk assessment requirements to controls

3.12 SECURITY ASSESSMENT

Basic Security Requirements

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.[26]

Derived Security Requirements

None.

Mapping security assessment requirements to controls

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements

3.13.1 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.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Derived Security Requirements

3.13.3 Separate user functionality from system management functionality.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

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

[26] There is no prescribed format or specified level of detail for *system security plans*. However, organizations ensure that the required information in 3.12.4 is conveyed in those plans.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.7 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).

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.12 Prohibit remote activation[27] of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.13 Control and monitor the use of mobile code.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.15 Protect the authenticity of communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

Mapping system and communications protection requirements to controls

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements

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

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

3.14.3 Monitor system security alerts and advisories and take action in response.

Derived Security Requirements

3.14.4 Update malicious code protection mechanisms when new releases are available.

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7 Identify unauthorized use of organizational systems.

Mapping system and information integrity requirements to controls

[27] 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.

	ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
3.1.6	**SECURITY REQUIREMENT** Use non-privileged accounts or roles when accessing nonsecurity functions.
	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.
3.1.7	**SECURITY REQUIREMENT** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
	DISCUSSION Privileged functions include, for example, 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 intrusion 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.
3.1.8	**SECURITY REQUIREMENT** Limit unsuccessful logon attempts.
	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 the application levels.
3.1.9	**SECURITY REQUIREMENT** Provide privacy and security notices consistent with applicable CUI rules.
	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 an assessment of risk, 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 should consult with the Office of the General Counsel for legal review and approval of warning banner content.

3.1.10

SECURITY REQUIREMENT

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

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.

3.1.11

SECURITY REQUIREMENT

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

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, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

3.1.12

SECURITY REQUIREMENT

Monitor and control remote access sessions.

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, for example: 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 safeguards (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 Special Publications 800-46, 800-77, and 800-113 provide guidance on secure remote access and virtual private networks.

3.1.13	**SECURITY REQUIREMENT** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
	DISCUSSION Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See NIST Cryptographic Standards; NIST Cryptographic Module Validation Program; NIST Cryptographic Algorithm Validation Program; NSA Cryptographic Standards.
3.1.14	**SECURITY REQUIREMENT** Route remote access via managed access control points.
	DISCUSSION Routing all 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.
3.1.15	**SECURITY REQUIREMENT** Authorize remote execution of privileged commands and remote access to security-relevant information.
	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. 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.
3.1.16	**SECURITY REQUIREMENT** Authorize wireless access prior to allowing such connections.
	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. NIST Special Publications 800-48 and 800-97 provide guidance on secure wireless networks.

3.1.17	**SECURITY REQUIREMENT** Protect wireless access using authentication and encryption.
	DISCUSSION Organizations can authenticate individuals and devices to help protect wireless access to the system. Special attention should be given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See NIST Cryptographic Standards.
3.1.18	**SECURITY REQUIREMENT** Control connection of mobile devices.
	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, for example: configuration management; device identification and authentication; 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 safeguards for mobile devices are reflected in other CUI security requirements. NIST Special Publication 800-124 provides guidance on mobile device security.
3.1.19	**SECURITY REQUIREMENT** Encrypt CUI on mobile devices and mobile computing platforms.
	DISCUSSION Organizations can use 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, for example, encrypting selected data structures such as files, records, or fields. See NIST Cryptographic Standards.
3.1.20	**SECURITY REQUIREMENT** Verify and control/limit connections to and use of external systems.
	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 safeguards on those systems. External systems include, for example, personally owned systems 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 safeguards so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required safeguards have been implemented can be achieved, for example, 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.
3.1.21	**SECURITY REQUIREMENT** Limit use of portable storage devices on external systems.
	DISCUSSION Limits on the use of organization-controlled portable storage devices in external systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. 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.
3.1.22	**SECURITY REQUIREMENT** Control CUI posted or processed on publicly accessible systems.
	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.

TABLE F-2: DISCUSSION ON AWARENESS AND TRAINING REQUIREMENTS

3.2.1	**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.
	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 can include, for example, formal training, offering supplies inscribed with security reminders, generating email advisories or notices from organizational officials, displaying logon screen messages, displaying posters, and conducting information security awareness events. NIST Special Publication 800-50 provides guidance on security awareness and training programs.
3.2.2	**SECURITY REQUIREMENT** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
	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, system or network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards. Such training can include, for example, policies, procedures, tools, and artifacts for the organizational 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 Special Publication 800-181 provides guidance on role-based information security training in the workplace.
3.2.3	**SECURITY REQUIREMENT** Provide security awareness training on recognizing and reporting potential indicators of insider threat.
	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 organizational policies, procedures, directives, rules, or practices. 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).

TABLE F-3: DISCUSSION ON AUDIT AND ACCOUNTABILITY REQUIREMENTS

3.3.1	**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.
	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, for example, 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, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/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, for example, 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 Special Publication 800-92 provides guidance on security log management.
3.3.2	**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.
	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, for example, results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, use of maintenance tools, nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, system component inventory, communications at the system boundaries, use of mobile code, and use of VoIP.

3.3.3	**SECURITY REQUIREMENT** Review and update logged events.
	DISCUSSION The intent of this requirement is to periodically re-evaluate which of the logged events will continue to be included in the list of events to be logged. Over time, the event types that are logged by organizations may change. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.
3.3.4	**SECURITY REQUIREMENT** Alert in the event of an audit logging process failure.
	DISCUSSION Audit logging process failures include, for example, software/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.
3.3.5	**SECURITY REQUIREMENT** Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
	DISCUSSION Correlating these 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.
3.3.6	**SECURITY REQUIREMENT** Provide audit record reduction and report generation to support on-demand analysis and reporting.
	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.
3.3.7	**SECURITY REQUIREMENT** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
	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 Network Time Protocol.
3.3.8	**SECURITY REQUIREMENT** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
	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.
3.3.9	**SECURITY REQUIREMENT** Limit management of audit logging functionality to a subset of privileged users.
	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.

TABLE F-4: DISCUSSION ON CONFIGURATION MANAGEMENT REQUIREMENTS

3.4.1

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.

DISCUSSION

This requirement establishes baseline configurations for systems and system components including communications and connectivity aspects of systems. 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 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, for example, 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, for example, manufacturer, device type, model, serial number, and physical location.

NIST Special Publication 800-128 provides guidance on security-focused configuration management

3.4.2

SECURITY REQUIREMENT

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

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, for example, mainframe computers, servers, workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, devices, 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, for example: 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, for example, information technology product

	developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. NIST Special Publications 800-70 and 800-128 provide guidance on security configuration settings.
3.4.3	**SECURITY REQUIREMENT** Track, review, approve or disapprove, and log changes to organizational systems.
	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, for example, 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 Special Publication 800-128 provides guidance on configuration change control.
3.4.4	**SECURITY REQUIREMENT** Analyze the security impact of changes prior to implementation.
	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, for example, reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of safeguards and how specific changes might affect the safeguards. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional safeguards are required. NIST Special Publication 800-128 provides guidance on configuration change control and security impact analysis.
3.4.5	**SECURITY REQUIREMENT** Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
	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, for example, 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 specified times). In addition to security concerns, commonly-accepted due diligence for configuration

management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration.

NIST Special Publication 800-128 provides guidance on configuration change control.

3.4.6

SECURITY REQUIREMENT

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

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, but 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.

3.4.7

SECURITY REQUIREMENT

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

DISCUSSION

Restricting the use of nonessential software (programs) includes, for example, 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.

3.4.8

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.

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.

NIST Special Publication 800-167 provides guidance on application whitelisting.

3.4.9

SECURITY REQUIREMENT

Control and monitor user-installed software.

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, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, 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.

TABLE F-5: DISCUSSION ON IDENTIFICATION AND AUTHENTICATION REQUIREMENTS

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.
	DISCUSSION Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared 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 Special Publication 800-63 provides guidance on digital identities.
3.5.2	**SECURITY REQUIREMENT** Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
	DISCUSSION Individual authenticators include, for example, 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, for example, 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, for example, 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, for example, certificates and passwords. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.3	**SECURITY REQUIREMENT** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
	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 solutions that feature physical authenticators include, for example, 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

	network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information traversing the network. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.4	**SECURITY REQUIREMENT** Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
	DISCUSSION Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.5	**SECURITY REQUIREMENT** Prevent reuse of identifiers for a defined period.
	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.
3.5.6	**SECURITY REQUIREMENT** Disable identifiers after a defined period of inactivity.
	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.
3.5.7	**SECURITY REQUIREMENT** Enforce a minimum password complexity and change of characters when new passwords are created.
	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.
3.5.8	**SECURITY REQUIREMENT** Prohibit password reuse for a specified number of generations.
	DISCUSSION Password lifetime restrictions do not apply to temporary passwords.

3.5.9	**SECURITY REQUIREMENT** Allow temporary password use for system logons with an immediate change to a permanent password.
	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.
3.5.10	**SECURITY REQUIREMENT** Store and transmit only cryptographically-protected passwords.
	DISCUSSION Cryptographically-protected passwords include, for example, salted one-way cryptographic hashes of passwords. See NIST Cryptographic Standards.
3.5.11	**SECURITY REQUIREMENT** Obscure feedback of authentication information.
	DISCUSSION The feedback from systems does not provide 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, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

TABLE F-6: DISCUSSION ON INCIDENT RESPONSE REQUIREMENTS

3.6.1	**SECURITY REQUIREMENT** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
	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, for example, 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, for example, 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 Special Publication 800-61 provides guidance on incident handling. NIST Special Publications 800-86 and 800-101 provide guidance on integrating forensic techniques into incident response.
3.6.2	**SECURITY REQUIREMENT** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
	DISCUSSION Tracking and documenting system security incidents includes, for example, 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, for example, 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, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies. NIST Special Publication 800-61 provides guidance on incident handling.

3.6.3	**SECURITY REQUIREMENT** Test the organizational incident response capability.
	DISCUSSION Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. NIST Special Publication 800-84 provides guidance on testing programs for information technology capabilities.

TABLE F-7: DISCUSSION ON MAINTENANCE REQUIREMENTS

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	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.
3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
	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.
3.7.3	**SECURITY REQUIREMENT** Ensure equipment removed for off-site maintenance is sanitized of any CUI.
	DISCUSSION This control addresses the information security aspects of system maintenance that is performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement). NIST Special Publication 800-88 provides guidance on media sanitization.
3.7.4	**SECURITY REQUIREMENT** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	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.
3.7.5	**SECURITY REQUIREMENT** Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
	DISCUSSION Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. Authentication techniques used in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

3.7.6	**SECURITY REQUIREMENT** Supervise the maintenance activities of maintenance personnel without required access authorization.
	DISCUSSION This requirement applies to individuals 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.

TABLE F-8: DISCUSSION ON MEDIA PROTECTION REQUIREMENTS

3.8.1	**SECURITY REQUIREMENT** Protect (i.e. physically control and securely store) system media containing CUI, both paper and digital.
	DISCUSSION System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Protecting digital media includes, for example, 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, for example, 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, for example, 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, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices.
3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	DISCUSSION Access can be limited by physically controlling system media and secure storage. Physically controlling system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library.
3.8.3	**SECURITY REQUIREMENT** Sanitize or destroy system media containing CUI before disposal or release for reuse.
	DISCUSSION This requirement applies to all system media, digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, 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 media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information 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, for example, destruction, removing CUI from a document, 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 the sanitization process for controlled unclassified information.

	See NARA Sanitization Policy and Guidance. NIST Special Publication 800-88 provides guidance on media sanitization.
3.8.4	**SECURITY REQUIREMENT** Mark media with necessary CUI markings and distribution limitations.
	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 Marking Handbook.
3.8.5	**SECURITY REQUIREMENT** Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
	DISCUSSION Controlled areas are areas or spaces for which organizations provide physical or procedural safeguards to meet the requirements established for protecting systems and information. Safeguards to maintain accountability for media during transport include, for example, 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 from outside the organization. Maintaining accountability of media during transport includes, for example, 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.
3.8.6	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
	DISCUSSION This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices. See NIST Cryptographic Standards.
3.8.7	**SECURITY REQUIREMENT** Control the use of removable media on system components.
	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 safeguards (e.g., policies, procedures, 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, for example, 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, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.
3.8.8	**SECURITY REQUIREMENT** Prohibit the use of portable storage devices when such devices have no identifiable owner.
	DISCUSSION Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).
3.8.9	**SECURITY REQUIREMENT** Protect the confidentiality of backup CUI at storage locations.
	DISCUSSION Organizations can employ cryptographic mechanisms or alternative physical safeguards 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, for example, system-state information, operating system software and application software, and licenses. User-level information includes information other than system-level information.

TABLE F-9: DISCUSSION ON PERSONNEL SECURITY REQUIREMENTS

3.9.1	**SECURITY REQUIREMENT** Screen individuals prior to authorizing access to organizational systems containing CUI.
	DISCUSSION Personnel screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.
3.9.2	**SECURITY REQUIREMENT** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
	DISCUSSION Protecting CUI during and after personnel actions may include, for example, return of system-related property and exit interviews. System-related property includes, for example, 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, for example, 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, for example, returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

TABLE F-10: DISCUSSION ON PHYSICAL PROTECTION REQUIREMENTS

3.10.1	**SECURITY REQUIREMENT** Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	DISCUSSION This requirement applies to organizational employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials which include, for example, 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, for example, 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 hard disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.
3.10.2	**SECURITY REQUIREMENT** Protect and monitor the physical facility and support infrastructure for organizational systems.
	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 safeguards applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such safeguards may also be necessary to help prevent eavesdropping or modification of unencrypted transmissions. Safeguards used to control physical access to support infrastructure include, for example, locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.
3.10.3	**SECURITY REQUIREMENT** Escort visitors and monitor visitor activity.
	DISCUSSION Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.
3.10.4	**SECURITY REQUIREMENT** Maintain audit logs of physical access.
	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 and when such access occurred), 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. Components of systems (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

3.10.5	**SECURITY REQUIREMENT** Control and manage physical access devices.
	DISCUSSION Physical access devices include, for example, keys, locks, combinations, and card readers.
3.10.6	**SECURITY REQUIREMENT** Enforce safeguarding measures for CUI at alternate work sites.
	DISCUSSION Alternate work sites may include, for example, government facilities or private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. NIST Special Publications 800-46 and 800-114 provide guidance on enterprise and user security when teleworking.

TABLE F-11: DISCUSSION ON RISK ASSESSMENT REQUIREMENTS

3.11.1	**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 transmission of CUI.
	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. NIST Special Publication 800-30 provides guidance on conducting risk assessments.
3.11.2	**SECURITY REQUIREMENT** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	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, for example: 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 use the Open Vulnerability Assessment Language (OVAL) to determine the presence of 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 Special Publication 800-40 provides guidance on vulnerability management.

3.11.3	**SECURITY REQUIREMENT** Remediate vulnerabilities in accordance with risk assessments.
	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.

TABLE F-12: DISCUSSION ON SECURITY ASSESSMENT REQUIREMENTS

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	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 life cycle. NIST Special Publication 800-53A provides guidance on developing security assessment plans and for conducting assessments. NIST Special Publication 800-53 provides guidance on security and privacy controls for systems and organizations.
3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
	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. 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.
3.12.3	**SECURITY REQUIREMENT** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
	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 more effective and timely risk management decisions.

Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

NIST Special Publication 800-137 provides guidance on continuous monitoring.

3.12.4

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.

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 specific design or implementation of the controls. 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 Special Publication 800-18 provides guidance on developing security plans.

TABLE F-13: DISCUSSION ON SYSTEM AND COMMUNICATIONS PROTECTION REQUIREMENTS

3.13.1	**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.
	DISCUSSION Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include, for example, 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, for example, restricting external web 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 Special Publication 800-41 provides guidance on firewalls and firewall policy. NIST Special Publication 800-125 provides guidance on security for virtualization technologies.
3.13.2	**SECURITY REQUIREMENT** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
	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. NIST Special Publication 800-160 provides guidance on systems security engineering.
3.13.3	**SECURITY REQUIREMENT** Separate user functionality from system management functionality.
	DISCUSSION System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from 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, for example, 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.
3.13.4	**SECURITY REQUIREMENT** Prevent unauthorized and unintended information transfer via shared system resources.
	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.
3.13.5	**SECURITY REQUIREMENT** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
	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, for example, routers, gateways, firewalls, virtualization, or cloud-based technologies. NIST Special Publication 800-41 provides guidance on firewalls and firewall policy. NIST Special Publication 800-125 provides guidance on security for virtualization technologies.
3.13.6	**SECURITY REQUIREMENT** Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
	DISCUSSION This requirement applies to inbound and outbound network communications traffic, both 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.
3.13.7	**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).
	DISCUSSION Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling would allow 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,

	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.
3.13.8	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	DISCUSSION This requirement applies to internal and external networks and any system components that can transmit information including, for example, servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of a controlled boundary are susceptible to 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 needed safeguards for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in standard, 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 Cryptographic Standards.
3.13.9	**SECURITY REQUIREMENT** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
	DISCUSSION This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include, for example, 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, for example, time periods by type of network access or for specific network accesses.
3.13.10	**SECURITY REQUIREMENT** Establish and manage cryptographic keys for cryptography employed in organizational systems.
	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, directives, regulations, policies, and standards, specifying appropriate options, levels, and parameters. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key maintenance.

3.13.11	**SECURITY REQUIREMENT** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
	DISCUSSION Cryptography can be employed to support many security solutions including, for example, 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 NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on other security requirements, organizations define each type of cryptographic use and the type of cryptography required (e.g., FIPS-validated cryptography). See NIST Cryptographic Standards; NIST Cryptographic Module Validation Program; NIST Cryptographic Algorithm Validation Program.
3.13.12	**SECURITY REQUIREMENT** Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
	DISCUSSION Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Indication of use includes, for example, 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.
3.13.13	**SECURITY REQUIREMENT** Control and monitor the use of mobile code.
	DISCUSSION Mobile code technologies include, for example, 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, for example, requiring mobile code to be digitally signed by a trusted source. NIST Special Publication 800-28 provides guidance on mobile code.
3.13.14	**SECURITY REQUIREMENT** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
	DISCUSSION VoIP has different requirements, features, functionality, availability, and service limitations when compared with Plain Old Telephone Service (POTS) (i.e., the standard telephone service that most homes use). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

	NIST Special Publication 800-58 provides guidance on Voice Over IP Systems.
3.13.15	**SECURITY REQUIREMENT** Protect the authenticity of communications sessions.
	DISCUSSION Authenticity protection includes, for example, protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. NIST Special Publications 800-52, 800-77, 800-95, and 800-113 provide guidance on secure communications sessions.
3.13.16	**SECURITY REQUIREMENT** Protect the confidentiality of CUI at rest.
	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 employ other safeguards including, for example, 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 Cryptographic Standards.

TABLE F-14: DISCUSSION ON SYSTEM AND INFORMATION INTEGRITY REQUIREMENTS

3.14.1	**SECURITY REQUIREMENT** Identify, report, and correct system flaws in a timely manner.
	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, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases 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, for example, 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 Special Publication 800-40 provides guidance on patch management technologies.
3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.
	DISCUSSION Designated locations include system entry and exit points which may include, for example, firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes, for example, 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, for example, 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, for example, 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, for example, 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, for example, 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 Special Publication 800-83 provides guidance on malware incident prevention.
3.14.3	**SECURITY REQUIREMENT** Monitor system security alerts and advisories and take action in response.
	DISCUSSION 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.
3.14.4	**SECURITY REQUIREMENT** Update malicious code protection mechanisms when new releases are available.
	DISCUSSION Malicious code protection mechanisms include, for example, 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, for example, 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, for example, 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.
3.14.5	**SECURITY REQUIREMENT** Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
	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, for example, 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, for example, 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, for example, 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, for example, 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.
3.14.6	**SECURITY REQUIREMENT** Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
	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, for example, 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 and outbound communications traffic include, for example, 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 Special Publication 800-94 provides guidance on intrusion detection and prevention systems.

3.14.7

SECURITY REQUIREMENT

Identify unauthorized use of organizational systems.

DISCUSSION

System monitoring can detect unauthorized use of organizational systems. System monitoring includes external and internal monitoring. System monitoring is an integral part of continuous monitoring and incident response programs; it 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 or unauthorized activities or conditions related to inbound and outbound communications traffic include, for example, 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 Special Publication 800-94 provides guidance on intrusion detection and prevention systems.