Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date May 14, 2024

Original Release Date November 9, 2023

The attached draft document is followed by:

Status Final

Series/Number NIST SP 800-171r3

Title Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Publication Date May 2024

DOI https://doi.org/10.6028/NIST.SP.800-171r3

CSRC URL https://csrc.nist.gov/pubs/sp/800/171/r3/final

Additional Information

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-171r3 fpd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Final Public Draft

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3.fpd

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-171r3 fpd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Final Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3.fpd

November 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:

Ross R, Pillitteri V (2023) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3 fpd. https://doi.org/10.6028/NIST.SP.800-171r3.fpd

Author ORCID iDs

Ron Ross: 0000-0002-1099-9757
Victoria Pillitteri: 0000-0002-7446-7506

Public Comment Period

November 9, 2023 – January 26, 2024 (originally Jan. 12, 2024)

Submit Comments

800-171comments@list.nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations. The requirements apply to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Keywords

Controlled Unclassified Information; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; nonfederal organizations; nonfederal systems; organization-defined parameter; security assessment; security control; security requirement.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Audience

This publication serves a diverse group of individuals and organizations in the public and private sectors, including:

- Federal agencies responsible for managing and protecting CUI
- Nonfederal organizations responsible for protecting CUI
- Individuals with system development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Individuals with acquisition or procurement responsibilities (e.g., contracting officers)
- Individuals with system, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Individuals with security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, analysts, independent verifiers and validators)

The above roles and responsibilities can be viewed from two perspectives:

- *Federal perspective*: The entity establishing and conveying the security requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with the security requirements set forth in contracts or agreements

Note to Reviewers

This update to NIST Special Publication (SP) 800-171, Revision 3 includes the changes made to the initial public draft (ipd) in response to the public comments received. Many trade-offs have been made to ensure that the technical and non-technical requirements have been stated clearly and concisely while also recognizing the specific needs of federal and nonfederal organizations. The following significant changes have been made to the initial public draft of NIST SP 800-171, Revision 3:

- Eliminated the NFO control tailoring category
- Introduced a new control tailoring category for controls that are addressed by other related controls (ORC)
- Eliminated selected organization-defined parameters (ODPs) where the ODP specification did not significantly impact the security requirement
- Clarified the responsibility for assigning ODP values
- Combined security requirements (or parts of requirements) with other requirements for consistency and ease of use
- Added security requirements due to control categorization changes
- Sequenced the content in the discussion sections to align with the individual parts of the requirements
- Modified the tailoring categories of selected controls and control items (subparts of controls)
- Added leading zeros to security requirement numbers to achieve greater consistency with SP 800-171A numbering formats and to support automated tool usage

Information regarding the transition of security requirements from NIST SP 800-171, Revision 2 to Revision 3 can be found on the publication details web page.

Reviewers are encouraged to comment on all or parts of draft NIST SP 800-171, Revision 3. NIST requests that comments be submitted to 800-171comments@list.nist.gov by 11:59 p.m. Eastern Standard Time (EST) on **January 12, 2024**. Commenters are encouraged to use the comment template provided with the document announcement.

Comments received in response to this request will be posted on the Protecting CUI project site after the due date. Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: 800-171comments@list.nist.gov

Table of Contents

List of Tables

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors whose constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura, Isabel Van Wyk, and Cristina Ritfeld – for their outstanding support in preparing this document for publication. Finally, a special note of thanks goes out to Kelley Dempsey for the initial research and development of the technical content used in the prototype CUI overlay.

Historical Contributions

The authors also wish to acknowledge the following organizations and individuals for their historic contributions to this publication:

- *Organizations:* National Archives and Records Administration, Department of Defense
- *Individuals:* Carol Bales, Matthew Barrett, Jon Boyens, Devin Casey, Christian Enloe, Gary Guissanie, Peggy Himes, Robert Glenn, Elizabeth Lennon, Vicki Michetti, Dorian Pappas, Karen Quigg, Mark Riddle, Matthew Scholl, Mary Thomas, Murugiah Souppaya, Patricia Toth, and Patrick Viscuso

1. Introduction

Executive Order (EO) 13556 [1] established a governmentwide program to standardize the way the executive branch handles Controlled Unclassified Information (CUI).[1] EO 13556 required that the CUI program emphasize openness, transparency, and uniformity of governmentwide practices and that the program implementation take place in a manner consistent with Office of Management and Budget (OMB) policies and National Institute of Standards and Technology (NIST) standards and guidelines. As the CUI program Executive Agent, the National Archives and Records Administration (NARA) provides information, guidance, policy, and requirements on handling CUI [4]. This includes approved CUI categories and descriptions, the basis for safeguarding and dissemination controls, and procedures for the use of CUI.[2] The CUI federal regulation [5] provides guidance to federal agencies on the designation, safeguarding, marking, dissemination, decontrolling, and disposition of CUI; establishes self-inspection and oversight requirements; and delineates other facets of the program.

The CUI regulation requires federal agencies that use federal information systems[3] to process, store, or transmit CUI to comply with NIST standards and guidelines. The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal organizations.[4] Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems.[5] To maintain a consistent level of protection, the security requirements for safeguarding CUI in nonfederal systems and organizations must comply with FIPS 199 [6] and FIPS 200 [7]. The requirements are derived from the controls in NIST Special Publication (SP) 800-53 [8].

1.1. Purpose and Applicability

The purpose of this publication is to provide federal agencies with recommended security requirements[6] for protecting the *confidentiality* of CUI[7] when such information is resident in nonfederal systems and organizations and where there are no specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI registry [4]. The requirements do not apply to nonfederal organizations that are collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency.[8]

[1] CUI is any information that a law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under EO 13526 [2], or any predecessor or successor order, or the Atomic Energy Act [3] as amended.

[2] Procedures for the use of CUI include marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

[3] A *federal information system* is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. The term *system* is used in this publication to represent people, processes, and technologies involved in the processing, storage, or transmission of CUI. Systems can include operational technology (OT), information technology (IT), Internet of Things (IoT) devices, Industrial IoT (IIoT) devices, specialized systems, cyber-physical systems, embedded systems, and sensors.

[4] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system.

[5] A *nonfederal system* is any system that does not meet the criteria for a federal information system.

[6] The term *security requirement* refers to the protection needs for a system or organization. Security requirements may be derived from laws, Executive Orders, directives, regulations, policies, standards, mission and business needs, or risk assessments.

[7] In accordance with EO 13526 [2] and 32 CFR 2002 [5], the scope of CUI protection is primarily focused on *confidentiality*. However, the security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms support both objectives. Therefore, the security requirements in this publication address the protection of CUI from unauthorized disclosure and modification.

[8] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency must comply with the requirements in FISMA [9].

The security requirements in this publication are *only* applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components.[9] The requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations.

Appropriately scoping requirements is an important factor in determining protection-related investment decisions and managing security risks for nonfederal organizations. If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for CUI and avoid increasing the organization's security posture beyond what it requires for protecting its missions, operations, and assets.

1.2. Organization of This Publication

The remainder of this special publication is organized as follows:

- Section 2 describes the assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI, the format of the requirements, and the tailoring criteria applied to the NIST standards and guidelines to obtain the requirements.
- Section 3 lists the security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.

The following sections provide additional information to support the protection of CUI in nonfederal systems and organizations:

- References
- Appendix A: Acronyms
- Appendix B: Glossary
- Appendix C: Tailoring Criteria
- Appendix D: Change Log

[9] System *components* include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, and applications.

2. The Fundamentals

This section describes the basic assumptions and methodology used to develop the requirements to protect the confidentiality of CUI in nonfederal systems and organizations. It also includes the tailoring[10] criteria applied to the controls in NIST SP 800-53 [8].

2.1. Basic Assumptions

The security requirements in this publication are based on the following assumptions:

- Federal information designated as CUI has the same value, whether such information resides in a federal or a nonfederal system or organization.
- Statutory and regulatory requirements for the protection of CUI are consistent in federal and nonfederal systems and organizations.
- Safeguards implemented to protect CUI are consistent in federal and nonfederal systems and organizations.
- The confidentiality impact value for CUI is no less than *moderate*.[11]
- Nonfederal organizations can directly implement a variety of potential security solutions or use external service providers to satisfy security requirements.

2.2. Security Requirement Development Methodology

Starting with the NIST SP 800-53 controls in the NIST SP 800-53B [12] moderate baseline, the controls are *tailored* to eliminate selected controls or parts of controls that are:

- Primarily the responsibility of the Federal Government;
- Not directly related to protecting the confidentiality of CUI;
- Adequately addressed by other related controls;[12] or
- Not applicable.

The NIST SP 800-171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of CUI. The security requirements are organized into 17 families, as illustrated in Table 1. Each family contains the requirements related to the general security topic of the family. Certain families from NIST SP 800-53 are not included due to the aforementioned tailoring criteria.[13]

[10] *Tailoring* is the process by which control baselines are modified to achieve certain organizational goals and objectives [13].

[11] FIPS 199 [6] defines three confidentiality impact values: low, moderate, and high. In accordance with 32 CFR 2002 [5], CUI is categorized at no less than the moderate confidentiality impact value. However, when federal law, regulation, or governmentwide policy establishing the control of CUI specifies controls that differ from those of the moderate confidentiality baseline, then the applicable law, regulation, or governmentwide policy is followed.

[12] "Adequately addressed by other related controls" means that the protection capability offered by the control is provided by another control in the same or different control family. Using this tailoring option helps to eliminate potential redundancy in requirements without affecting the protection of CUI in nonfederal systems and organizations.

[13] The PII Processing and Transparency (PT) family is not included because PII is a category of CUI, and therefore, no additional requirements are specified for confidentiality protection. The Program Management (PM) family is not included because it is not associated with any security control baseline.

Table 1. Security requirement families

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

Organization-defined parameters (ODPs) are included for some requirements. These ODPs provide flexibility through the use of *assignment* and *selection* operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements.[14] Assignment and selection operations provide the capability to customize the security requirements based on specific protection needs. The determination of organization-defined parameter values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, the values for the organization-defined parameters become part of the requirement.

A *discussion* section is included with each requirement. It is derived from the control discussion sections in NIST SP 800-53 and provides additional information to facilitate the implementation and assessment of the requirements. The discussion section is informative, not normative. It is not intended to extend the scope of a requirement or to influence the solutions that organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive and not reflective of potential options available to organizations. A *references* section provides the source controls from NIST SP 800-53 and a list of NIST Special Publications with additional information on the topic described in the security requirement.[15]

The structure and content of a typical security requirement is provided in the example below:

3.13.11 Cryptographic Protection

REQUIREMENT: 03.13.11

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

REFERENCES

Source Control: SC-13
Supporting Publications: FIPS 140-3 [38]

[14] NIST does not establish or assign values for ODPs. If ODP values for selected security requirements are not formally established or assigned by a federal agency or a consortium of federal agencies, nonfederal organizations assign those values to complete the requirements.

[15] Unless specified in federal policy, the guidance in supporting NIST publications in the references section is *informative*, not *normative*.

ORGANIZATION-DEFINED PARAMETERS

Organization-defined parameters are an important part of a security requirement specification. ODPs provide the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, technologies, operational environments, and risk tolerance. ODPs also support consistent security assessments in determining whether specified security requirements have been satisfied.

The term *organization* is used in many security requirements. The meaning of the term is context dependent. For example, in a security requirement with an ODP, an organization can refer to either the federal agency or the nonfederal organization establishing the parameter values for the requirement.

Appendix C describes the security control tailoring criteria used to develop the CUI security requirements and the results of the tailoring process. The appendix provides a list of controls from NIST SP 800-53 that support the requirements and the controls that have been eliminated from the moderate baseline in accordance with the tailoring criteria.

3. The Requirements

This section describes 17 families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations. When used in the context of the requirements in Section 3, the term *system* is narrowed to only include nonfederal systems or system components that process, store, or transmit CUI or that provide protection for such systems or components. Not all security requirements mention CUI explicitly. However, the requirements are included because they directly affect the protection of CUI during processing, while in storage, and when in transmission between different locations.

Some systems, including specialized systems (e.g., industrial/process control systems, medical devices, computer numerical control machines), may have limitations on the application of certain security requirements. To accommodate such issues, the system security plan — as reflected in requirement 03.15.02 — is used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies are managed though organizational plans of action and milestones, as reflected in requirement 03.12.02.

3.1. Access Control

3.1.1. Account Management

REQUIREMENT: 03.01.01

a. Define the types of system accounts allowed and prohibited.

b. Create, enable, modify, disable, and remove system accounts in accordance with organizational policy, procedures, prerequisites, and criteria.

c. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges).

d. Authorize access to the system based on a valid access authorization and intended system usage.

e. Monitor the use of system accounts.

f. Disable system accounts when:

   1. The accounts have expired;
   2. The accounts have been inactive for [*Assignment: organization-defined time period*];
   3. The accounts are no longer associated with a user or individual;
   4. The accounts are in violation of organizational policy; or
   5. Significant risks associated with individuals are discovered.

g. Notify organizational personnel or roles when:

   1. Accounts are no longer required;
   2. Users are terminated or transferred; and
   3. System usage or need-to-know changes for an individual.

DISCUSSION

This requirement focuses on account management for systems and applications. The definition and enforcement of access authorizations other than those determined by account type (e.g., privileged access, non-privileged access) are addressed in requirement 03.01.02. System account types include individual, group, temporary, system, guest, anonymous, emergency, developer, and service. Users who require administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access. Types of accounts that organizations may prohibit due to increased risk include group, emergency, guest, anonymous, and temporary.

Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of both. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system requirements (e.g., system upgrades, scheduled maintenance) and mission and business requirements (e.g., time zone differences, remote access to facilitate travel requirements).

Users who pose a significant security risk include individuals for whom reliable evidence indicates either the intention to use authorized access to the system to cause harm or that adversaries will cause harm through them. Close coordination among human resource managers, mission/business owners, system administrators, and legal staff is essential when disabling system accounts for high-risk individuals. Time periods for the notification of organizational personnel or roles may vary.

REFERENCES

Source Controls: AC-02, AC-02(03), AC-02(13)
Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

3.1.2. Access Enforcement

REQUIREMENT: 03.01.02

Enforce approved authorizations for logical access to CUI and system resources.

DISCUSSION

Access control policies control access between active entities or subjects (i.e., users or system processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. Types of system access include remote access and access to systems that communicate through external networks, such as the internet. Access enforcement mechanisms can also be employed at the application and service levels to provide increased protection for CUI. This recognizes that the system can host many applications and services in support of mission and business functions.

REFERENCES

Source Control: AC-03
Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

3.1.3. Information Flow Enforcement

REQUIREMENT: 03.01.03

Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

DISCUSSION

Information flow control regulates where CUI can transit within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include keeping CUI from being transmitted in the clear to the internet, blocking outside traffic that claims to be from within the organization, restricting requests to the internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.

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

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

REFERENCES

Source Control: AC-04
Supporting Publications: SP 800-160-1 [11], SP 800-162 [22], SP 800-178 [23]

3.1.4. Separation of Duties

REQUIREMENT: 03.01.04

a. Identify the duties of individuals requiring separation.

b. Define system access authorizations to support separation of duties.

DISCUSSION

Separation of duties addresses the potential for abuse of authorized privileges and reduces the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and support functions among different individuals or roles, conducting system support functions

with different individuals or roles (e.g., quality assurance, configuration management, system management, assessments, programming, and network security), and ensuring that personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of their systems and system components when developing policies on separation of duties. This requirement is enforced by 03.01.02.

REFERENCES

Source Control: AC-05
Supporting Publications: SP 800-162 [22], SP 800-178 [23]

3.1.5. Least Privilege

REQUIREMENT: 03.01.05

a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.

b. Authorize access to [*Assignment: organization-defined security functions and security-relevant information*].

c. Review the privileges assigned to roles or classes of users periodically to validate the need for such privileges.

d. Reassign or remove privileges, as necessary.

DISCUSSION

Organizations employ the principle of least privilege for specific duties and authorized access for users and system processes. Least privilege is applied to the development, implementation, and operation of the system. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Security functions include establishing system accounts and assigning privileges, installing software, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, and establishing intrusion detection parameters. Security-relevant information includes threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, security architecture, cryptographic key management information, and access control lists.

REFERENCES

Source Controls: AC-06, AC-06(01), AC-06(07), AU-09(04)
Supporting Publications: None

3.1.6. Least Privilege – Privileged Accounts

REQUIREMENT: 03.01.06

a. Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or roles*].

b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing nonsecurity functions or nonsecurity information.

DISCUSSION

Privileged accounts are typically described as system administrator accounts. Restricting privileged accounts to specific personnel or roles prevents nonprivileged users from accessing security functions or security-relevant information. Requiring the use of non-privileged accounts when accessing nonsecurity functions or nonsecurity information limits exposure when operating from within privileged accounts. Including roles addresses situations in which 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 the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

REFERENCES

Source Controls: AC-06(02), AC-06(05)
Supporting Publications: None

3.1.7. Least Privilege – Privileged Functions

REQUIREMENT: 03.01.07

a. Prevent non-privileged users from executing privileged functions.

b. Log the execution of privileged functions.

DISCUSSION

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users do not possess the appropriate authorizations to execute privileged functions. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. This requirement represents a condition to be achieved by the definition of authorized privileges in 03.01.01 and the enforcement of those privileges in 03.01.02.

The misuse of privileged functions – whether intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts – is a serious and ongoing concern that can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse and mitigate the risks from insider threats and advanced persistent threats.

REFERENCES

Source Controls: AC-06(09), AC-06(10)
Supporting Publications: None

3.1.8. Unsuccessful Logon Attempts

REQUIREMENT: 03.01.08

Limit the number of consecutive invalid logon attempts to [*Assignment: organization-defined number*] in [*Assignment: organization-defined time period*].

DISCUSSION

Due to the potential for denial of service, automatic system lockouts are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., using a delay algorithm). Organizations may employ different delay algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful system logon attempts may be implemented at the system and application levels.

REFERENCES

Source Control: AC-07
Supporting Publications: SP 800-63-3 [27], SP 800-124 [28]

3.1.9. System Use Notification

REQUIREMENT: 03.01.09

Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.

DISCUSSION

System use notifications can be implemented using warning or banner messages. The messages are displayed before individuals log in to the system. System use notifications are used for access via logon interfaces with human users and are not required when human interfaces do not exist. Organizations consider whether a secondary use notification is needed to access applications or other system resources after the initial network logon. Posters or other printed materials may be used in lieu of an automated system message. This requirement is related to 03.15.03.

REFERENCES

Source Control: AC-08
Supporting Publications: None

3.1.10. Device Lock

REQUIREMENT: 03.01.10

a. Prevent access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*].

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

DISCUSSION

Device locks are temporary actions taken to prevent access to the system when users depart from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or application level. User-initiated device locking is behavior- or policy-based and requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of the system, such as when organizations require users to log out at the end of

workdays. Pattern-hiding displays can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

REFERENCES

Source Controls: AC-11, AC-11(01)
Supporting Publications: None

3.1.11. Session Termination

REQUIREMENT: 03.01.11

Terminate a user session automatically after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

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) in 03.13.09. A logical session is initiated whenever a user (or processes acting on behalf of a user) accesses a system. Logical sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination ends all system processes associated with a user's logical session except those processes that are created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic session termination can include organization-defined periods of user inactivity, time-of-day restrictions on system use, and targeted responses to certain types of incidents.

REFERENCES

Source Control: AC-12
Supporting Publications: None

3.1.12. Remote Access

REQUIREMENT: 03.01.12

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

b. Authorize each type of remote system access prior to establishing such connections.

c. Route remote access to the system through authorized and managed access control points.

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

DISCUSSION

Remote access to the system represents a significant potential vulnerability that can be exploited by adversaries. Monitoring and controlling remote access methods allows organizations to detect attacks and ensure compliance with remote access policies. This occurs by auditing the connection activities of remote users on the systems. Routing remote access through managed access control points enhances explicit control over such connections and reduces susceptibility to unauthorized access to the system, which could result in the unauthorized disclosure of CUI.

Restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and its susceptibility to threats by adversaries. A privileged command is a human-initiated command executed on a system that involves the control, monitoring, or administration of the system, including security functions and security-relevant information. Security-relevant information is information 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 access from remote locations helps to ensure that unauthorized individuals are unable to execute such commands with the potential to do serious or catastrophic damage to the system.

REFERENCES

Source Controls: AC-17, AC-17(03), AC-17(04)
Supporting Publications: SP 800-46 [14], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], IR 7966 [26]

3.1.13. Withdrawn

Incorporated into 03.01.12.

3.1.14. Withdrawn

Incorporated into 03.01.12.

3.1.15. Withdrawn

Incorporated into 03.01.12.

3.1.16. Wireless Access

REQUIREMENT: 03.01.16

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.

b. Authorize each type of wireless access to the system prior to establishing such connections.

c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.

DISCUSSION

Establishing usage restrictions, configuration requirements, and connection requirements for wireless access to the system provides criteria to support access authorization decisions. These restrictions and requirements reduce susceptibility to unauthorized system access through wireless technologies. Wireless networks use authentication protocols that provide credential protection and mutual authentication. Organizations authenticate individuals and devices to protect wireless access to the system. Special attention is given to the variety of devices with potential wireless access to the system, including small form factor mobile devices (e.g., smart phones, smart watches). Wireless networking capabilities that are embedded within system

components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential missions or business functions can help reduce susceptibility to threats by adversaries involving wireless technologies.

REFERENCES

Source Controls: AC-18, AC-18(03)
Supporting Publications: SP 800-94 [29], SP 800-97 [30], SP 800-124 [28]

3.1.17. Withdrawn

Incorporated into 03.01.16.

3.1.18. Access Control for Mobile Devices

REQUIREMENT: 03.01.18

a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.

b. Authorize the connection of mobile devices to the system.

c. Implement full-device or container-based encryption to protect the confidentiality of CUI on 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; possesses local, non-removable, or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, smart watches, and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of mobile devices may be comparable to or a subset of notebook or desktop systems, depending on the nature and intended purpose of the device. The protection and control of mobile devices is behavior- or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which the organization provides physical or procedural controls to meet the requirements established for protecting CUI.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions, configuration requirements, and connection requirements for mobile devices include configuration management, device identification and authentication, implementing mandatory protective software, 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. Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices. Container-based encryption provides a fine-grained approach to the encryption of data and information, including encrypting selected data structures (e.g., files, records, or fields).

REFERENCES

Source Controls: AC-19, AC-19(05)
Supporting Publications: SP 800-46 [14], SP 800-114 [31], SP 800-124 [28]

3.1.19. Withdrawn

Incorporated into 03.01.18.

3.1.20. Use of External Systems

REQUIREMENT: 03.01.20

a. Prohibit the use of external systems unless the systems are specifically authorized.

b. Establish the following terms, conditions, and security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [*Assignment: organization-defined terms, conditions, and requirements*].

c. Permit authorized individuals to use an external system to access the organizational system or to process, store, or transmit CUI only after:

   1. Verification of the implementation of security requirements on the external system as specified in the organization's security plans; and

   2. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

DISCUSSION

External systems are systems that are used by but are not part of the organization. External systems include personally owned systems, system components, or devices; privately owned computing and communication devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; and systems managed by contractors. Organizations have the option to prohibit the use of any type of external system or specified types of external systems, (e.g., prohibit the use of external systems that are not organizationally owned). Terms and conditions are consistent with the trust relationships established with the entities that own, operate, or maintain external systems and include descriptions of shared responsibilities.

Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to the organizational system and over whom organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on the trust relationships between organizations. Organizations need assurance that the external systems satisfy the necessary security requirements so as not to compromise, damage, or harm the system. This requirement is related to 03.16.03.

REFERENCES

Source Controls: AC-20, AC-20(01), AC-20(02)
Supporting Publications: None

3.1.21. Withdrawn

Incorporated into 03.01.20.

3.1.22. Publicly Accessible Content

REQUIREMENT: 03.01.22

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

b. Review the content on publicly accessible systems for CUI periodically and remove such information, if discovered.

DISCUSSION

In accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including CUI.

REFERENCES

Source Control: AC-22
Supporting Publications: None

3.2. Awareness and Training

3.2.1. Literacy Training and Awareness

REQUIREMENT: 03.02.01

a. Provide security literacy training to system users:

1. As part of initial training for new users and periodically thereafter;
2. When required by system changes or following [*Assignment: organization-defined events*]; and
3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.

b. Update security literacy training content periodically and following [*Assignment: organization-defined events*].

DISCUSSION

Organizations provide basic and advanced levels of security literacy training to system users (including managers, senior executives, system administrators, and contractors) and measures to test the knowledge level of users. Organizations determine the content of literacy training based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and the actions required of users to maintain security and to respond to incidents. The content also addresses the need for operations security and the handling of CUI.

Security awareness techniques include displaying posters, offering supplies inscribed with security reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events using podcasts, videos, and

webinars. Security literacy training is conducted at a frequency consistent with applicable laws, directives, regulations, and policies. Updating literacy training content on a regular basis ensures that the content remains relevant. Events that may precipitate an update to literacy training content include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

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

Social engineering is an attempt to deceive an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, threadjacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Security literacy training includes how to communicate employee and management concerns regarding potential indicators of insider threat and potential and actual instances of social engineering and data mining through appropriate organizational channels in accordance with established policies and procedures.

REFERENCES

Source Controls: AT-02, AT-02(02), AT-02(03)
Supporting Publications: SP 800-50 [32], SP 800-160-2 [10]

3.2.2. Role-Based Training

REQUIREMENT: 03.02.02

a. Provide role-based security training to organizational personnel:

   1. Before authorizing access to the system or CUI, before performing assigned duties, and periodically thereafter; and

   2. When required by system changes or following [*Assignment: organization-defined events*].

b. Update role-based training content periodically and following [*Assignment: organization-defined events*].

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 the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, software developers, systems integrators, acquisition/procurement officials, system and network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and personnel with access to system-level software with security-related technical training specifically tailored for their assigned duties.

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

REFERENCES

Source Control: AT-03
Supporting Publications: SP 800-161 [33], SP 800-181 [34]

3.2.3. Withdrawn

Incorporated into 03.02.01.

3.3. Audit and Accountability

3.3.1. Event Logging

REQUIREMENT: 03.03.01

a. Specify the following event types selected for logging within the system: [*Assignment: organization-defined event types*].

b. Review and update the event types selected for logging periodically.

DISCUSSION

An event is any observable occurrence in a system, including unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed. This includes events that are relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, the execution of privileged functions, failed logons or accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the system monitoring and auditing that are appropriate for each of the security requirements. When defining event types, organizations consider 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. 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. The event types that are logged by organizations may change over time. Periodically reviewing and updating the set of logged event types is necessary to ensure that the current set remains necessary and sufficient.

REFERENCES

Source Control: AU-02
Supporting Publications: SP 800-92 [35]

3.3.2. Audit Record Content

REQUIREMENT: 03.03.02

a. Include the following content in audit records:
   1. What type of event occurred;
   2. When the event occurred;
   3. Where the event occurred;
   4. Source of the event;
   5. Outcome of the event; and
   6. Identity of individuals, subjects, objects, or entities associated with the event.

b. Provide additional information for audit records, as needed.

DISCUSSION

Audit record content that may be necessary to support the auditing function includes time stamps, source and destination addresses, user or process identifiers, event descriptions, file names, and the access control or flow control rules that are 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 a full text recording of privileged commands or the individual identities of group account users.

REFERENCES

Source Controls: AU-03, AU-03(01)
Supporting Publications: None

3.3.3. Audit Record Generation

REQUIREMENT: 03.03.03

a. Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02.

b. Retain audit records for a time period consistent with records retention policy.

DISCUSSION

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. The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records, including the access control or flow control rules invoked and the individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements.

REFERENCES

Source Controls: AU-11, AU-12
Supporting Publications: SP 800-92 [35]

3.3.4. Response to Audit Logging Process Failures

REQUIREMENT: 03.03.04

a. Alert organizational personnel or roles within [*Assignment: organization-defined time period*] in the event of an audit logging process failure.

b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

DISCUSSION

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Response actions include overwriting the oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

REFERENCES

Source Control: AU-05
Supporting Publications: None

3.3.5. Audit Record Review, Analysis, and Reporting

REQUIREMENT: 03.03.05

a. Review and analyze system audit records periodically for indications and potential impact of inappropriate or unusual activity.

b. Report findings to organizational personnel or roles.

c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

DISCUSSION

Audit record review, analysis, and reporting cover information security logging performed by organizations and can include logging that results from the monitoring of account usage, remote access, wireless connectivity, configuration settings, the use of maintenance tools and nonlocal maintenance, system component inventory, mobile device connection, equipment delivery and removal, physical access, temperature and humidity, communications at system interfaces, and the use of mobile code. Findings can be reported to organizational entities, such as the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The scope, frequency, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received. Correlating audit record review, analysis, and reporting processes helps to ensure that they collectively create a more complete view of events. The requirement to assess a given system is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

706 **REFERENCES**

707 Source Controls: AU-06, AU-06(03)
708 Supporting Publications: SP 800-86 [36], SP 800-101 [37]

709 ## 3.3.6. Audit Record Reduction and Report Generation

710 **REQUIREMENT:** 03.03.06

711 a. Implement an audit record reduction and report generation capability that supports audit
712 record review, analysis, reporting requirements, and after-the-fact investigations of incidents.

713 b. Preserve the original content and time ordering of audit records.

714 **DISCUSSION**

715 Audit records are generated in 03.03.03. Audit record reduction and report generation occur after
716 audit record generation. Audit record reduction is a process that manipulates collected audit
717 information and organizes it in a summary format that is more meaningful to analysts. Audit
718 record reduction and report generation capabilities do not always come from the same system or
719 organizational entities that conduct auditing activities. An audit record reduction capability can
720 include, for example, modern data mining techniques with advanced data filters to identify
721 anomalous behavior in audit records. The report generation capability provided by the system can
722 help generate customizable reports. The time ordering of audit records can be a significant issue if
723 the granularity of the time stamp in the record is insufficient.

724 **REFERENCES**

725 Source Control: AU-07
726 Supporting Publications: None

727 ## 3.3.7. Time Stamps

728 **REQUIREMENT:** 03.03.07

729 a. Use internal system clocks to generate time stamps for audit records.

730 b. Record time stamps for audit records that meet [*Assignment: organization-defined granularity*
731 *of time measurement*] and that:

732 1. Use Coordinated Universal Time (UTC);

733 2. Have a fixed local time offset from UTC; or

734 3. Include the local time offset as part of the time stamp.

735 **DISCUSSION**

736 Time stamps generated by the system include the date and time. Time is commonly expressed in
737 Coordinated Universal Time (UTC) – a modern continuation of Greenwich Mean Time (GMT) –
738 or local time with an offset from UTC. The granularity of time measurements refers to the degree
739 of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within
740 hundreds or tens of milliseconds). Organizations may define different time granularities for
741 system components. Time service can be critical to other security capabilities, such as access
742 control, and identification and authentication, depending on the nature of the mechanisms used to
743 support those capabilities.

REFERENCES

Source Control: AU-08
Supporting Publications: None

3.3.8. Protection of Audit Information

REQUIREMENT: 03.03.08

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

b. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.

DISCUSSION

Audit information includes the information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are programs and devices used to conduct audit and logging activities. The protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. The physical protection of audit information is addressed by media and physical protection requirements.

Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

REFERENCES

Source Controls: AU-09, AU-09(04)
Supporting Publications: None

3.3.9. Withdrawn

Incorporated into 03.03.08.

3.4. Configuration Management

3.4.1. Baseline Configuration

REQUIREMENT: 03.04.01

a. Develop and maintain under configuration control, a current baseline configuration of the system.

b. Review and update the baseline configuration of the system periodically and when system components are installed or modified.

DISCUSSION

Baseline configurations for the system and system components include aspects of connectivity, operation, and communications. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for the system or configuration items within the system. Baseline

configurations serve as a basis for future builds, releases, or changes to the system and include information about system components, operational procedures, network topology, and the placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as the system changes over time. Baseline configurations of the system reflect the current enterprise architecture.

REFERENCES

Source Control: CM-02
Supporting Publications: SP 800-124 [28], SP 800-128 [41], IR 8011-2 [42], IR 8011-3 [43]

3.4.2. Configuration Settings

REQUIREMENT: 03.04.02

a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [*Assignment: organization-defined configuration settings*].

b. Identify, document, and approve any deviations from established configuration settings.

DISCUSSION

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

Security parameters are those parameters that impact the security state of the system, including the parameters required to satisfy other security requirements. Security parameters include registry settings; account, file, and directory permission settings (i.e., privileges); and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for the system. The established settings become part of the system's configuration baseline.

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

REFERENCES

Source Control: CM-06
Supporting Publications: SP 800-70 [44], SP 800-126 [45], SP 800-128 [41]

3.4.3. Configuration Change Control

REQUIREMENT: 03.04.03

a. Define the types of changes to the system that are configuration-controlled.

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts.

c. Implement and document approved configuration-controlled changes to the system.

d. Monitor and review activities associated with configuration-controlled changes to the system.

DISCUSSION

Configuration change control refers to tracking, reviewing, approving or disapproving, and logging changes to the system. Specifically, it involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the system, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for system components (e.g., operating systems, applications, firewalls, routers, mobile devices) and configuration items of the system, changes to configuration settings, unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

REFERENCES

Source Control: CM-03
Supporting Publications: SP 800-124 [28], SP 800-128 [41]

3.4.4. Impact Analyses

REQUIREMENT: 03.04.04

Analyze the security impact of changes to the system prior to implementation.

DISCUSSION

Organizational personnel with security responsibilities conduct impact analyses that include reviewing security plans, policies, and procedures to understand security requirements; reviewing system design documentation and operational procedures to understand how system changes might affect the security state of the system; reviewing the impacts of changes on supply chain partners with stakeholders; and determining how potential changes to a system create new risks and the ability to mitigate those risks. Impact analyses also include risk assessments to understand the impacts of changes and to determine whether additional security requirements are needed.

REFERENCES

Source Control: CM-04
Supporting Publications: SP 800-128 [41]

3.4.5. Access Restrictions for Change

REQUIREMENT: 03.04.05

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

DISCUSSION

Changes to the hardware, software, or firmware components of the system or the operational procedures related to the system can have potentially significant effects on the security of the system. Therefore, organizations permit only qualified and authorized individuals to access the

system for the purpose of initiating changes. Access restrictions include physical and logical access controls, software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into the system), and change windows (i.e., changes occur only during specified times).

REFERENCES

Source Control: CM-05
Supporting Publications: FIPS 140-3 [38], FIPS 180-4 [39], SP 800-128 [41]

3.4.6. Least Functionality

REQUIREMENT: 03.04.06

a. Configure the system to provide only mission-essential capabilities.

b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [*Assignment: organization-defined functions, ports, protocols, connections, and services*].

c. Review the system periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

DISCUSSION

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

Organizations review the functions and services provided by the system or system components to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent the unauthorized connection of devices, transfer of information, and tunneling. Organizations can employ network scanning tools, intrusion detection and prevention systems, and endpoint protection systems (e.g., firewalls and host-based intrusion detection systems) to identify and prevent the use of prohibited functions, ports, protocols, system connections, and services. Bluetooth, File Transfer Protocol, and peer-to-peer networking are examples of the types of protocols that organizations consider eliminating, restricting, or disabling.

REFERENCES

Source Controls: CM-07, CM-07(01)
Supporting Publications: SP 800-160-1 [11], SP 800-167 [46]

3.4.7. Withdrawn

Incorporated into 03.04.06.

3.4.8. Authorized Software – Allow by Exception

REQUIREMENT: 03.04.08

a. Identify software programs authorized to execute on the system.

b. Implement a deny-all, allow-by-exception policy for the execution of software programs on the system.

c. Review and update the list of authorized software programs periodically.

DISCUSSION

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

Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection against attacks that bypass application-level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. The verification of authorized software can occur either prior to execution or at system startup.

REFERENCES

Source Control: CM-07(05)
Supporting Publications: SP 800-160-1 [11], SP 800-167 [46]

3.4.9. Withdrawn

Addressed by 03.01.05, 03.01.06, 03.01.07, and 03.04.08.

3.4.10. System Component Inventory

REQUIREMENT: 03.04.10

a. Develop and document an inventory of system components.

b. Review and update the system component inventory periodically.

c. Update the system component inventory as part of installations, removals, and system updates.

DISCUSSION

System components are discrete, identifiable assets (i.e., hardware, software, and firmware elements) that compose a system. Organizations may implement centralized system component inventories that include components from all systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the

system name, software owners, software version numbers, hardware inventory specifications, software license information — and for networked components — the machine names and network addresses for all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include component type, physical location, date of receipt, manufacturer, cost, model, serial number, and supplier information.

REFERENCES

Source Controls: CM-08, CM-08(01)
Supporting Publications: SP 800-124 [28], SP 800-128 [41], IR 8011-2 [42], IR 8011-3 [43]

3.4.11. Information Location

REQUIREMENT: 03.04.11

a. Identify and document the location of CUI and the system components on which the information is processed and stored.

b. Identify and document the users who have access to the system and system components where CUI is processed and stored.

c. Document changes to the location (i.e., system or system components) where CUI is processed and stored.

DISCUSSION

Information location addresses the need to understand the specific system components where CUI is being processed and stored and the users who have access to CUI so that appropriate protection mechanisms can be provided, including information flow controls, access controls, and information management.

REFERENCES

Source Control: CM-12
Supporting Publications: None

3.4.12. System and Component Configuration for High-Risk Areas

REQUIREMENT: 03.04.12

a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [*Assignment: organization-defined system configurations*].

b. Apply the following security requirements to the system or system components when the individuals return from travel: [*Assignment: organization-defined security requirements*].

DISCUSSION

When it is known that a system or a specific system component will be in a high-risk area, additional security requirements may be needed to counter the increased threat. Organizations can implement protective measures on systems or system components used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that the components are configured as intended before travel is initiated, and taking additional actions after travel is completed. For example, systems going into high-risk areas can be configured with sanitized hard drives, limited applications, and more stringent configuration settings. Actions applied to

mobile devices upon return from travel include examining the device for signs of physical tampering and purging and reimaging the device storage.

REFERENCES

Source Control: CM-02(07)
Supporting Publications: SP 800-124 [28], SP 800-128 [41]

3.5. Identification and Authentication

3.5.1. User Identification, Authentication, and Re-Authentication

REQUIREMENT: 03.05.01

a. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users.

b. Re-authenticate users when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

DISCUSSION

System users include individuals (or system processes acting on behalf of individuals) who are authorized to access a system. Typically, individual identifiers are the usernames associated with the system accounts assigned to those individuals. Since system processes execute on behalf of groups and roles, organizations may require the unique identification of individuals in group accounts or accountability of individual activity. The unique identification and authentication of users applies to all system accesses. Organizations employ passwords, physical authenticators, biometrics, or some combination thereof to authenticate user identities. Organizations may re-authenticate individuals in certain situations, including when roles, authenticators, or credentials change; when the execution of privileged functions occurs; after a fixed time period; or periodically.

REFERENCES

Source Controls: IA-02, IA-11
Supporting Publications: SP 800-63-3 [27]

3.5.2. Device Identification and Authentication

REQUIREMENT: 03.05.02

Uniquely identify and authenticate devices before establishing a system connection.

DISCUSSION

Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to

identify and authenticate devices on local and wide area networks. PKI and certificate revocation checking for the certificates exchanged can also be included as part of device authentication.

REFERENCES

Source Control: IA-03
Supporting Publications: SP 800-63-3 [27]

3.5.3. Multi-Factor Authentication

REQUIREMENT: 03.05.03

Implement multi-factor authentication for access to system accounts.

DISCUSSION

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator, such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level to provide increased information security.

REFERENCES

Source Controls: IA-02(01), IA-02(02)
Supporting Publications: SP 800-63-3 [27]

3.5.4. Replay-Resistant Authentication

REQUIREMENT: 03.05.04

Implement replay-resistant authentication mechanisms for access to system 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 protocols that use nonces or challenges, such as time synchronous or challenge-response one-time authenticators.

REFERENCES

Source Control: IA-02(08)
Supporting Publications: SP 800-63-3 [27]

3.5.5. Identifier Management

REQUIREMENT: 03.05.05

a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

b. Select and assign an identifier that identifies an individual, group, role, service, or device.

c. Prevent reuse of identifiers for [*Assignment: organization-defined time period*].

d. Uniquely identify the status of each individual with an identifying characteristic.

DISCUSSION

Identifiers are provided for users, processes acting on behalf of users, and devices. Prohibiting the reuse of identifiers prevents the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices. Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides useful information about the people with whom organizational personnel are communicating. For example, is useful for an employee to know that one of the individuals on an email message is a contractor.

REFERENCES

Source Controls: IA-04, IA-04(04)
Supporting Publications: SP 800-63-3 [27]

3.5.6. Withdrawn

3.5.7. Password Management

REQUIREMENT: 03.05.07

a. Maintain a list of commonly-used, expected, or compromised passwords and update the list periodically and when organizational passwords are suspected to have been compromised.

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords.

c. Transmit passwords only over cryptographically-protected channels.

d. Store passwords in a cryptographically-protected form.

e. Select a new password upon first use after account recovery.

f. Enforce the following composition and complexity rules for passwords: [*Assignment: organization-defined composition and complexity rules*].

DISCUSSION

Password-based authentication applies to passwords used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable to shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length) under certain circumstances and can enforce this requirement. For example, account recovery can occur when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof. 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 and

reduces the susceptibility to authenticator compromises. Long passwords and passphrases can be used to increase the complexity of passwords.

REFERENCES

Source Control: IA-05(01)
Supporting Publications: SP 800-63-3 [27]

3.5.8. Withdrawn

3.5.9. Withdrawn

Incorporated into 03.05.07.

3.5.10. Withdrawn

Incorporated into 03.05.07.

3.5.11. Authentication Feedback

REQUIREMENT: 03.05.11

Obscure feedback of authentication information during the authentication process.

DISCUSSION

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

REFERENCES

Source Control: IA-06
Supporting Publications: None

3.5.12. Authenticator Management

REQUIREMENT: 03.05.12

a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.
b. Establish initial authenticator content for any authenticators issued by the organization.
c. Establish and implement administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators.
d. Change default authenticators at first use.

e. Change or refresh authenticators periodically or when the following events occur: [*Assignment: organization-defined events*].

f. Protect authenticator content from unauthorized disclosure and modification.

DISCUSSION

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. The initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, requirements for authenticator content contain specific characteristics. Authenticator management is supported by organization-defined settings and restrictions for various authenticator characteristics (e.g., password complexity and composition rules, validation time window for time synchronous one-time tokens, and the number of allowed rejections during the verification stage of biometric authentication).

The requirement to protect individual authenticators may be implemented by 03.15.03 for authenticators in the possession of individuals and by 03.01.01, 03.01.02, 03.01.05, and 03.13.08 for authenticators stored in organizational systems. This includes passwords stored in hashed or encrypted formats or files that contain encrypted or hashed passwords accessible with administrator privileges. Actions can be taken to protect authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Developers may deliver 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 risk. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed. The use of long passwords or passphrases may obviate the need to periodically change authenticators.

REFERENCES

Source Control: IA-05
Supporting Publications: SP 800-63-3 [27]

3.6. Incident Response

3.6.1. Incident Response Plan and Handling

REQUIREMENT: 03.06.01

a. Develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability.

b. Implement an incident-handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

DISCUSSION

It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. Incident-related information can be obtained from a variety of sources, including audit monitoring, network monitoring, physical access monitoring, user and

administrator reports, and reported supply chain events. An effective incident handling capability involves coordination among many organizational entities, including mission and business owners, system owners, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.

REFERENCES

Source Controls: IR-04, IR-08
Supporting Publications: SP 800-50 [32], SP 800-61 [47], SP 800-161 [33]

3.6.2. Incident Monitoring, Reporting, and Response Assistance

REQUIREMENT: 03.06.02

a. Track and document system security incidents.

b. Report suspected incidents to the organizational incident response capability within [*Assignment: organization-defined time period*].

c. Report incident information to [*Assignment: organization-defined authorities*].

d. Provide an incident response support resource that offers advice and assistance to users of the system for the handling and reporting of incidents.

DISCUSSION

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from many sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. 3.6.1 provides information on the types of incidents that are appropriate for monitoring. The types of incidents reported, the content and timeliness of the reports, and the reporting authorities reflect applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Incident information informs risk assessments, the effectiveness of security assessments, the security requirements for acquisitions, and the selection criteria for technology products. Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensic services or consumer redress services, when required.

REFERENCES

Source Controls: IR-05, IR-06, IR-07
Supporting Publications: SP 800-61 [47], SP 800-86 [36]

3.6.3. Incident Response Testing

REQUIREMENT: 03.06.03

Test the effectiveness of the incident response capability periodically.

DISCUSSION

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations. Incident response testing can include a

determination of the effects of incident response on organizational operations, organizational assets, and individuals. Qualitative and quantitative data can help determine the effectiveness of incident response processes.

REFERENCES

Source Control: IR-03
Supporting Publications: SP 800-84 [48]

3.6.4. Incident Response Training

REQUIREMENT: 03.06.04

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
    1. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility or acquiring system access;
    2. When required by system changes; and
    3. Periodically thereafter.
b. Review and update incident response training content periodically and following [*Assignment: organization-defined events*].

DISCUSSION

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know whom to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of 03.02.02. Events that may precipitate an update to incident response training content include incident response plan testing, response to an actual incident, audit or assessment findings, or changes in applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

REFERENCES

Source Control: IR-02
Supporting Publications: SP 800-86 [36], SP 800-137 [49]

3.7. Maintenance

3.7.1. Withdrawn

Recategorized as NCO.

3.7.2. Withdrawn

Incorporated into 03.07.04 and 03.07.06.

3.7.3. Withdrawn

Incorporated into 03.08.03.

3.7.4. Maintenance Tools

REQUIREMENT: 03.07.04

a. Approve, control, and monitor the use of system maintenance tools.

b. Inspect the maintenance tools for improper or unauthorized modifications.

c. Check media containing diagnostic and test programs for malicious code before the media are used in the system.

d. Prevent the removal of system maintenance equipment containing CUI by:

   1. Verifying that there is no CUI on the equipment;

   2. Sanitizing or destroying the equipment; or

   3. Retaining the equipment within the facility.

DISCUSSION

Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with the tools that are used for diagnostic and repair actions on the system. Maintenance tools can include hardware and software diagnostic and test equipment as well as packet sniffers. The tools may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Diagnostic and test programs are potential vehicles for transporting malicious code into the system, either intentionally or unintentionally. Examples of media inspection include checking the cryptographic hash or digital signatures of diagnostic and test programs and/or media. If organizations inspect media that contain diagnostic and test programs and determine that the media also contains malicious code, the incident is handled consistent with incident handling policies and procedures. A periodic review of maintenance tools can result in the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools do not address the hardware and software components that support maintenance and are considered a part of the system (including software implementing utilities such as “ping,” “ls,” “ipconfig,” or hardware and software that implement the monitoring port of an Ethernet switch).

REFERENCES

Source Controls: MA-03, MA-03(01), MA-03(02), MA-03(03)
Supporting Publications: SP 800-88 [50]

3.7.5. Nonlocal Maintenance

REQUIREMENT: 03.07.05

a. Approve and monitor nonlocal maintenance and diagnostic activities.

b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.

c. Terminate session and network connections when nonlocal maintenance is completed.

DISCUSSION

Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the requirements in 03.05.01.

REFERENCES

Source Control: MA-04
Supporting Publications: SP 800-63-3 [27], SP 800-88 [50]

3.7.6. Maintenance Personnel

REQUIREMENT: 03.07.06

a. Establish a process for maintenance personnel authorization.
b. Maintain a list of authorized maintenance organizations or personnel.
c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.
d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

DISCUSSION

Maintenance personnel refers to individuals who perform hardware or software maintenance on the system, while 03.10.01 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the system. The technical competence of supervising individuals relates to the maintenance performed on the system, while having required access authorizations refers to maintenance on and near the system. Individuals who have not been previously identified as authorized maintenance personnel (e.g., manufacturers, consultants, systems integrators, and vendors) may require privileged access to the system, such as when they are required to conduct maintenance with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on their risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

REFERENCES

Source Control: MA-05
Supporting Publications: None

3.8. Media Protection

3.8.1. Media Storage

REQUIREMENT: 03.08.01

Physically control and securely store system media containing CUI until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

DISCUSSION

System media includes digital and non-digital media. Digital media includes diskettes, flash drives, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, establishing procedures to allow individuals to check out and return media to libraries, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. Controlled areas provide physical and procedural controls to meet the requirements established for protecting information and systems. Sanitization techniques (e.g., cryptographically erasing, destroying, clearing, and purging) prevent the disclosure of CUI to unauthorized individuals. The sanitization process removes CUI from media such that the information cannot be retrieved or reconstructed.

REFERENCES

Source Control: MP-04
Supporting Publications: SP 800-111 [51]

3.8.2. Media Access

REQUIREMENT: 03.08.02

Restrict access to CUI on system media.

DISCUSSION

System media includes digital and non-digital media. Access to CUI on system media can be restricted by physically controlling such media, which includes conducting inventories, ensuring that procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for stored media.

REFERENCES

Source Control: MP-02
Supporting Publications: SP 800-111 [51]

3.8.3. Media Sanitization

REQUIREMENT: 03.08.03

Sanitize system media containing CUI prior to disposal, release out of organizational control, or release for reuse.

DISCUSSION

Media sanitization applies to digital and non-digital media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, mobile devices, network components, and non-digital media. The sanitization process removes CUI from media such that the information cannot be retrieved or reconstructed. Sanitization techniques (e.g., cryptographically erasing, clearing, purging, and destroying) prevent the disclosure of CUI to unauthorized individuals when such media is reused or released for disposal. NARA policies control the sanitization process for media containing CUI and may require destruction when other methods cannot be applied to the media.

REFERENCES

Source Control: MP-06
Supporting Publications: SP 800-88 [50]

3.8.4. Media Marking

REQUIREMENT: 03.08.04

Mark system media containing CUI to indicate distribution limitations, handling caveats, and security markings.

DISCUSSION

System media includes digital and non-digital media. Security marking refers to the application or use of human-readable security attributes. Security labeling refers to the use of security attributes for internal system data structures. Digital media includes diskettes, magnetic tapes, external or removable solid state or magnetic drives, flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. CUI is defined by NARA along with marking, safeguarding, and dissemination requirements for such information.

REFERENCES

Source Control: MP-03
Supporting Publications: None

3.8.5. Media Transport

REQUIREMENT: 03.08.05

a. Protect and control system media containing CUI during transport outside of controlled areas.

b. Maintain accountability of system media containing CUI during transport outside of controlled areas.

DISCUSSION

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural measures to meet the requirements established for protecting information and systems. Media protection during transport can include cryptography and/or locked containers. Cryptographic mechanisms can provide confidentiality protections, depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. This requirement is related to 03.13.11.

REFERENCES

Source Controls: MP-05, SC-28, SC-28(01)
Supporting Publications: SP 800-111 [51]

3.8.6. Withdrawn

Incorporated into 03.08.05.

3.8.7. Media Use

REQUIREMENT: 03.08.07

a. Restrict or prohibit the use of [*Assignment: organization-defined types of system media*].

b. Prohibit the use of removable system media without an identifiable owner.

DISCUSSION

In contrast to requirement 03.08.01, which restricts user access to media, this requirement restricts the use of certain types of media, such as restricting or prohibiting the use of external hard drives, flash drives, or smart displays. This requirement also includes any potential restrictions on the use of removable system media in external systems. Organizations can use technical and non-technical measures (e.g., policies, procedures, and rules of behavior) to control the use of system media. For example, organizations may control the use of portable storage devices by using physical cages on workstations to prohibit access to external ports or disabling or removing the ability to insert, read, or write to devices.

Organizations may limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Organizations may also control the use of portable storage devices based on the type of device — prohibiting the use of writeable, portable devices — and implement this restriction by disabling or removing the capability to write to such devices. Limits on the use of organization-controlled system media in external systems include restrictions on how the media may be used and under what conditions. Requiring identifiable owners (e.g., individuals, organizations, or projects) for removable system media reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the media (e.g., insertion of malicious code).

REFERENCES

Source Control: MP-07
Supporting Publications: SP 800-111 [51]

3.8.8. Withdrawn

Incorporated into 03.08.07.

3.8.9. System Backup – Cryptographic Protection

REQUIREMENT: 03.08.09

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.

DISCUSSION

Backup storage locations may include system-level information and user-level information. System-level information includes system state information, operating system software,

application software, and licenses. User-level information includes information other than system-level information. Hardware-enabled security technologies (e.g., hardware security modules [HSM]) can be used to enhance cryptographic protection for backup information. HSM devices safeguard and manage cryptographic keys and provide cryptographic processing. Cryptographic operations (e.g., encryption, decryption, and signature generation/verification) are typically hosted on the HSM device, and many implementations provide hardware-accelerated mechanisms for cryptographic operations. This requirement is related to 03.13.11.

REFERENCES

Source Control: CP-09(08)
Supporting Publications: SP 800-34 [52], SP 800-130 [53], SP 800-152 [54]

3.9. Personnel Security

3.9.1. Personnel Screening

REQUIREMENT: 03.09.01

a. Screen individuals prior to authorizing access to the system.

b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening*].

DISCUSSION

Personnel security screening activities involve the assessment of an individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the individual's trustworthiness) prior to authorizing access to the system or when elevating system access. The screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and criteria established for the level of access required for the assigned position.

REFERENCES

Source Control: PS-03
Supporting Publications: SP 800-181 [34]

3.9.2. Personnel Termination and Transfer

REQUIREMENT: 03.09.02

a. When individual employment is terminated:

   1. Disable system access within [*Assignment: organization-defined time period*];
   2. Terminate or revoke authenticators and credentials associated with the individual; and
   3. Retrieve security-related system property.

b. When individuals are reassigned or transferred to other positions in the organization:

   1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility;
   2. Initiate [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the transfer or reassignment action*]; and

3. Modify access authorization to correspond with any changes in operational need.

DISCUSSION

Security-related system property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that accountability is achieved for the organizational property. Security topics at exit interviews include reminding individuals of potential limitations on future employment and nondisclosure agreements. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment.

The timely execution of termination actions is essential for individuals who have been terminated for cause. Organizations may consider disabling the accounts of individuals who are being terminated prior to the individuals being notified. This requirement applies to the reassignment or transfer of individuals when the personnel action is permanent or of such extended duration as to require protection. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new identification cards, keys, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing access to official records to which individuals had access at previous work locations in previous system accounts.

REFERENCES

Source Controls: PS-04, PS-05
Supporting Publications: None

3.10. Physical Protection

3.10.1. Physical Access Authorizations

REQUIREMENT: 03.10.01

a. Develop, approve, and maintain a list of individuals with authorized access to the physical location where the system resides.

b. Issue authorization credentials for physical access.

c. Review the physical access list periodically.

d. Remove individuals from the physical access list when access is no longer required.

DISCUSSION

A facility can include one or more physical locations containing systems or system components that process, store, or transmit CUI. Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include identification badges, identification cards, and smart cards. Organizations determine the strength of the authorization credentials consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

REFERENCES

Source Control: PE-02
Supporting Publications: None

3.10.2. Monitoring Physical Access

REQUIREMENT: 03.10.02

a. Monitor physical access to the location where the system resides to detect and respond to physical security incidents.

b. Review physical access logs periodically.

DISCUSSION

A facility can include one or more physical locations containing systems or system components that process, store, or transmit CUI. Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls if the access logs are part of an automated system. Incident response capabilities include investigations of physical security incidents and responses to those incidents. Incidents include security violations or suspicious physical access activities, such as access outside of normal work hours, repeated access to areas not normally accessed, access for unusual lengths of time, and out-of-sequence access.

REFERENCES

Source Control: PE-06
Supporting Publications: None

3.10.3. Withdrawn

Incorporated into 03.10.07.

3.10.4. Withdrawn

Incorporated into 03.10.07.

3.10.5. Withdrawn

Incorporated into 03.10.07.

3.10.6. Alternate Work Site

REQUIREMENT: 03.10.06

a. Determine alternate work sites allowed for use by employees.

b. Employ the following security requirements at alternate work sites: [*Assignment: organization-defined security requirements*].

DISCUSSION

Alternate work sites include the private residences of employees or other facilities designated by the organization. Alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different security requirements for specific alternate work sites or types of sites, depending on the work-related activities conducted at the sites. Assessing the effectiveness of the requirements and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

REFERENCES

Source Control: PE-17
Supporting Publications: SP 800-46 [14], SP 800-114 [20]

3.10.7. Physical Access Control

REQUIREMENT: 03.10.07

a. Control physical access at the location where the system resides by:
   1. Verifying individual physical access authorizations before granting access; and
   2. Controlling ingress and egress with physical access control systems/devices or guards.
b. Maintain physical access audit logs for entry or exit points.
c. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*].
d. Secure keys, combinations, and other physical access devices.

DISCUSSION

This requirement addresses physical locations containing systems or system components that process, store, or transmit CUI. Organizations determine the types of guards needed, including professional security staff or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include exterior access points, interior access points to systems that require supplemental access controls, or both. Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors.

REFERENCES

Source Control: PE-03
Supporting Publications: None

3.10.8. Access Control for Transmission and Output Devices

REQUIREMENT: 03.10.08

a. Control physical access to system distribution and transmission lines in organizational facilities.
b. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.

DISCUSSION

Safeguarding measures applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such measures may also be necessary to prevent eavesdropping or the modification of unencrypted transmissions. Safeguarding measures used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protecting cabling with conduit or cable trays, and wiretapping sensors. Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

REFERENCES

Source Controls: PE-04, PE-05
Supporting Publications: None

3.11. Risk Assessment

3.11.1. Risk Assessment

REQUIREMENT: 03.11.01

a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.

b. Update risk assessments periodically.

DISCUSSION

Establishing the system boundary is a prerequisite to assessing the risk of unauthorized disclosure of CUI. Risk assessments consider threats, vulnerabilities, likelihood, and adverse impacts to organizational operations and assets based on the operation and use of the system and the unauthorized disclosure of CUI. Risk assessments also consider risks from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing systems, outsourcing entities). Risk assessments 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. Risk assessments include supply chain-related risks associated with suppliers or contractors and the system, system component, or system service that they provide.

REFERENCES

Source Controls: RA-03, RA-03(01), SR-06
Supporting Publications: SP 800-30 [55], SP 800-161 [33]

3.11.2. Vulnerability Monitoring and Scanning

REQUIREMENT: 03.11.02

a. Monitor and scan for vulnerabilities in the system periodically and when new vulnerabilities affecting the system are identified.

b. Remediate system vulnerabilities within [*Assignment: organization-defined response times*].

c. Update system vulnerabilities to be scanned periodically and when new vulnerabilities are identified and reported.

DISCUSSION

Organizations determine the required vulnerability scanning for system components and ensure that potential sources of vulnerabilities (e.g., networked printers, scanners, and copiers) are not overlooked. Vulnerability analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, or binary analysis. Organizations can use these approaches in source code reviews and tools (e.g., static analysis tools, web-based application scanners, binary analyzers). Vulnerability scanning includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated and that employ the Extensible Configuration Checklist Description Format (XCCDF). Organizations also consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL). Sources for vulnerability information also include the Common Weakness Enumeration (CWE) listing, the National Vulnerability Database (NVD), and the Common Vulnerability Scoring System (CVSS).

REFERENCES

Source Controls: RA-05, RA-05(02)
Supporting Publications: SP 800-40 [56], SP 800-53A [57], SP 800-70 [44], SP 800-115 [58], SP 800-126 [45]

3.11.3. Withdrawn

Incorporated into 03.11.02.

3.12. Security Assessment and Monitoring

3.12.1. Security Assessment

REQUIREMENT: 03.12.01

Assess the security requirements for the system and its environment of operation periodically to determine if the requirements have been satisfied.

DISCUSSION

By assessing the security requirements, organizations determine whether the necessary safeguards and countermeasures are implemented correctly, operating as intended, and producing the desired outcome. Security assessments identify weaknesses and deficiencies in the system and provide the essential information needed to make risk-based decisions. Security assessment reports document assessment results in sufficient detail as deemed necessary by the organization to determine the accuracy and completeness of the reports. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

REFERENCES

Source Control: CA-02
Supporting Publications: SP 800-53 [8], SP 800-53A [57], SP 800-37 [59], SP 800-115 [58]

3.12.2. Plan of Action and Milestones

REQUIREMENT: 03.12.02

a. Develop a plan of action and milestones for the system:
   1. To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments; and
   2. To reduce or eliminate known system vulnerabilities.

b. Update the existing plan of action and milestones periodically based on the findings from security assessments, independent audits or reviews, and continuous monitoring activities.

DISCUSSION

Plans of action and milestones (POAMs) are important documents in organizational security programs. Organizations use POAMs to describe how unsatisfied security requirements will be met and how planned mitigations will be implemented. Organizations can document system security plans and POAMs as separate or combined documents and in any format. Federal agencies may consider system security plans and POAMs as inputs to risk-based decisions on whether to process, store, or transmit CUI on a system hosted by a nonfederal organization.

REFERENCES

Source Control: CA-05
Supporting Publications: SP 800-37 [59]

3.12.3. Continuous Monitoring

REQUIREMENT: 03.12.03

Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.

DISCUSSION

Continuous monitoring at the system level facilitates ongoing awareness of the system security posture to support risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess and monitor their systems at a frequency that is sufficient to support risk-based decisions. Different types of security requirements may require different monitoring frequencies.

REFERENCES

Source Control: CA-07
Supporting Publications: SP 800-37 [59], SP 800-39 [60], SP 800-53A [57], SP 800-115 [58], SP 800-137 [49]

3.12.4. Withdrawn

Incorporated into 03.15.02.

3.12.5. Information Exchange

REQUIREMENT: 03.12.05

a. Approve and manage the exchange of CUI between the system and other systems using [*Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements*].

b. Document, as part of the exchange agreements, interface characteristics, security requirements, and responsibilities for each system.

c. Review and update the exchange agreements periodically.

DISCUSSION

The types of agreements selected are based on factors such as the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual) and the level of access to the organizational system by users of the other system. Types of agreements can include interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service-level agreements, or other types of agreements. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (e.g., service providers, contractors, system developers, and system integrators). Examples of the types of information contained in exchange agreements include the interface characteristics, security requirements, controls, and responsibilities for each system.

REFERENCES

Source Control: CA-03
Supporting Publications: SP 800-47 [83]

3.13. System and Communications Protection

3.13.1. Boundary Protection

REQUIREMENT: 03.13.01

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.

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

c. Connect to external systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

DISCUSSION

Managed interfaces include gateways, routers, firewalls, network-based malicious code analysis, virtualization systems, and encrypted tunnels implemented within a security architecture. Subnetworks that are either physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses.

REFERENCES

Source Control: SC-07
Supporting Publications: SP 800-41 [64], SP 800-125B [65], SP 800-160-1 [11], SP 800-189 [67], SP 800-207 [66]

3.13.2. Withdrawn

Recategorized as NCO.

3.13.3. Withdrawn

Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, 03.01.07.

3.13.4. Information in Shared System Resources

REQUIREMENT: 03.13.04

Prevent unauthorized and unintended information transfer via shared system resources.

DISCUSSION

Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or actions of processes acting on behalf of prior users or roles) from being available to 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. Information in shared system resources also applies to encrypted representations of information. In other contexts, the control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted, covert channels (including storage and timing channels) in which shared system resources are manipulated to violate information flow restrictions, or components within systems for which there are only single users or roles.

REFERENCES

Source Control: SC-04
Supporting Publications: None

3.13.5. Withdrawn

Incorporated into 03.13.01.

3.13.6. Network Communications – Deny by Default – Allow by Exception

REQUIREMENT: 03.13.06

Deny network communications traffic by default and allow network communications traffic by exception.

DISCUSSION

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, allow-by-exception network communications traffic policy ensures that only essential and approved connections are allowed.

REFERENCES

Source Control: SC-07(05)
Supporting Publications: SP 800-41 [64], SP 800-77 [18], SP 800-189 [67]

3.13.7. Withdrawn

Addressed by 03.01.12, 03.04.02 and 03.04.06.

3.13.8. Transmission and Storage Confidentiality

REQUIREMENT: 03.13.08

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.

DISCUSSION

This requirement applies to internal and external networks and any system components that can transmit CUI, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are susceptible to interception and modification. Encryption protects CUI from unauthorized disclosure during transmission and while in storage. Cryptographic mechanisms that protect the confidentiality of CUI during transmission include TLS and IPsec. Information in storage (i.e., information at rest) refers to the state of CUI when it is not in process or in transit and resides on internal or external storage devices, storage area network devices, and databases. Protecting CUI in storage does not focus on the type of storage device or the frequency of access to that device but rather on the state of the information. This requirement relates to 03.13.11.

REFERENCES

Source Controls: SC-08, SC-08(01), SC-28, SC-28(01)
Supporting Publications: FIPS 140-3 [38], FIPS 197 [68], SP 800-46 [14], SP 800-52 [69], SP 800-56A [73], SP 800-56B [74], SP 800-56C [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-111 [51], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-124 [28], SP 800-177 [70]

3.13.9. Network Disconnect

REQUIREMENT: 03.13.09

Terminate network connections associated with communications sessions at the end of the sessions or after periods of inactivity.

DISCUSSION

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions includes deallocating TCP/IP addresses or port pairs at the operating system level or deallocating networking assignments at the application level if multiple application sessions are using a single network connection. Time periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

REFERENCES

Source Control: SC-10
Supporting Publications: None

3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key establishment and management*].

DISCUSSION

Cryptographic key establishment and management include key generation, distribution, storage, access, rotation, and destruction. Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to 03.13.11.

REFERENCES

Source Control: SC-12
Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]

3.13.11. Cryptographic Protection

REQUIREMENT: 03.13.11

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

REFERENCES

Source Control: SC-13

Supporting Publications: FIPS 140-3 [38]

3.13.12. Collaborative Computing Devices and Applications

REQUIREMENT: 03.13.12

a. Prohibit remote activation of collaborative computing devices and applications.

b. Provide an explicit indication of use to users physically present at the devices.

DISCUSSION

Collaborative computing devices include white boards, microphones, and cameras. Indication of use includes notifying users (e.g., a pop-up menu stating that recording is in progress, or that the microphone has been turned on) when collaborative computing devices are activated. Dedicated video conferencing systems, which typically rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded. Solutions to prevent device usage include webcam covers and buttons to disable microphones.

REFERENCES

Source Control: SC-15
Supporting Publications: None

3.13.13. Mobile Code

REQUIREMENT: 03.13.13

a. Define acceptable mobile code and mobile code technologies.

b. Authorize, monitor, and control the use of mobile code.

DISCUSSION

Mobile code includes software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. Decisions regarding the use of mobile code within the system are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, VBScript, and WebGL. Usage restrictions and implementation guidelines apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers, smart phones, and smart devices. Mobile code policy and procedures address the actions taken to prevent the development, acquisition, and use of unacceptable mobile code within the system, including requiring mobile code to be digitally signed by a trusted source.

REFERENCES

Source Control: SC-18
Supporting Publications: SP 800-28 [71]

3.13.14. Withdrawn

Technology-specific.

3.13.15. Session Authenticity

REQUIREMENT: 03.13.15

Protect the authenticity of communications sessions.

DISCUSSION

Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of the communications sessions in the ongoing identities of other parties and the validity of the transmitted information. Authenticity protection includes protecting against "adversary-in-the-middle" attacks, session hijacking, and the insertion of false information into sessions.

REFERENCES

Source Control: SC-23
Supporting Publications: SP 800-52 [69], SP 800-77 [18], SP 800-95 [72], SP 800-113 [19]

3.13.16. Withdrawn

Incorporated into 03.13.08.

3.14. System and Information Integrity

3.14.1. Flaw Remediation

REQUIREMENT: 03.14.01

a. Identify, report, and correct system flaws.

b. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates.

DISCUSSION

Organizations identify systems that are affected by announced software and firmware flaws, including potential vulnerabilities that result from those flaws, and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address the 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 the flaws discovered in organizational systems. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors, including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.

REFERENCES

Source Control: SI-02
Supporting Publications: SP 800-39 [60], SP 800-40 [56], SP 800-128 [41]

3.14.2. Malicious Code Protection

REQUIREMENT: 03.14.02

a. Implement malicious code protection mechanisms at designated locations within the system to detect and eradicate malicious code.

b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policy and procedures.

c. Configure malicious code protection mechanisms to:

1. Perform scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at endpoints or network entry and exit points as the files are downloaded, opened, or executed; and

2. Block malicious code, quarantine malicious code, or take other actions in response to malicious code detection.

DISCUSSION

Malicious code insertions occur through the exploitation of system vulnerabilities. Periodic scans of the system and real-time scans of files from external sources as files are downloaded, opened, or executed can detect malicious code. Malicious code can be inserted into the system in many ways, including by email, the Internet, and portable storage devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats, contained in compressed or hidden files, or hidden in files using techniques such as steganography. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software and custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

If malicious code cannot be detected by detection methods or technologies, organizations can rely on secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that the software only performs intended functions. Organizations may determine that different actions are warranted in response to the detection of malicious code. For example, organizations can define actions to be taken in response to malicious code detection during scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

REFERENCES

Source Control: SI-03
Supporting Publications: SP 800-83 [76], SP 800-125B [65], SP 800-177 [70]

3.14.3. Security Alerts, Advisories, and Directives

REQUIREMENT: 03.14.03

a. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.

b. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.

c. Implement security directives in accordance with established time frames.

DISCUSSION

There are many publicly available sources of system security alerts and advisories. For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) generate security alerts and advisories to maintain situational awareness across the Federal Government and in nonfederal organizations. Software vendors, subscription services, and industry Information Sharing and Analysis Centers (ISACs) may also provide security alerts and advisories. Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

REFERENCES

Source Control: SI-05
Supporting Publications: SP 800-161 [33]

3.14.4. Withdrawn

Incorporated into 03.14.02.

3.14.5. Withdrawn

Addressed by 03.14.02.

3.14.6. System Monitoring

REQUIREMENT: 03.14.06

a. Monitor the system to detect:
    1. Attacks and indicators of potential attacks; and
    2. Unauthorized connections.
b. Identify unauthorized use of the system.
c. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.

DISCUSSION

System monitoring involves external and internal monitoring. External monitoring includes the observation of events that occur at the system boundary. Internal monitoring includes the observation of events that occur within the system. Organizations can monitor the system, 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.

A system monitoring capability is achieved through a variety of tools and techniques (e.g., audit record monitoring software, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms that support critical applications with such devices being employed at managed system interfaces.

The granularity of monitoring the information collected is based on organizational monitoring objectives and the capability of the system to support such objectives.

Systems connections can be network, remote, or local. A network connection is any connection with a device that communicates through a network (e.g., local area network, the internet). A remote connection is any connection with a device that communicates through an external network (e.g., the internet). Network, remote, and local connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in the system or propagating among system components, the unauthorized export of information, or signaling to external systems. Evidence of malicious code is used to identify a potentially compromised system. System monitoring requirements, including the need for types of system monitoring, may be referenced in other requirements.

REFERENCES

Source Controls: SI-04, SI-04(04)
Supporting Publications: SP 800-61 [47], SP 800-83 [76], SP 800-92 [35], SP 800-94 [29], SP 800-137 [49], SP 800-177 [70]

3.14.7. Withdrawn

Incorporated into 03.14.06.

3.14.8. Information Management and Retention

REQUIREMENT: 03.14.08

Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

DISCUSSION

Federal agencies consider data retention requirements for nonfederal organizations. Retaining CUI on nonfederal systems after contracts or agreements have concluded increases the attack surface for those systems and the risk of the information being compromised. NARA provides federal policy and guidance on records retention and schedules.

REFERENCES

Source Control: SI-12
Supporting Publications: None

3.15. Planning

3.15.1. Policy and Procedures

REQUIREMENT: 03.15.01

a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.

b. Review and update policies and procedures periodically.

DISCUSSION

This requirement addresses policies and procedures for the protection of CUI. Policies and procedures contribute to security assurance and should address each family of the CUI security requirements. Policies can be included as part of the generalized organizational security policy or be represented by separate policies that address each family of requirements. Procedures describe how policies are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security plans or in one or more separate documents.

REFERENCES

Source Controls: AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01, SR-01
Supporting Publications: SP 800-12 [61], SP 800-100 [62]

3.15.2. System Security Plan

REQUIREMENT: 03.15.02

a. Develop a system security plan that:
   1. Defines the constituent system components;
   2. Describes the system operating environment;
   3. Describes specific threats to the system that are of concern to the organization;
   4. Provides an overview of the security requirements for the system;
   5. Identifies connections to other systems;
   6. Identifies individuals that fulfill system roles and responsibilities; and
   7. Includes other relevant information necessary for the protection of CUI.

b. Review and update the system security plan periodically.

c. Protect the system security plan from unauthorized disclosure.

DISCUSSION

System security plans provide key characteristics of the system that is processing, storing, and transmitting CUI and how the system and information are protected. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and the subsequent determinations of risk if the plan is implemented as intended. System security plans can be a collection of documents, including documents that already exist. Effective system security plans make use of references to policies, procedures, and additional documents (e.g., design specifications) where detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security information in other established management or operational areas related to enterprise architecture, the system development life cycle, systems engineering, and acquisition.

REFERENCES

Source Control: PL-02

Supporting Publications: SP 800-18 [63]

3.15.3. Rules of Behavior

REQUIREMENT: 03.15.03

a. Establish and provide to individuals requiring access to the system, rules that describe their responsibilities and expected behavior for handling CUI and system usage.

b. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.

c. Review and update the rules of behavior periodically.

DISCUSSION

Rules of behavior represent a type of access agreement for system users. Organizations consider rules of behavior for the handling of CUI based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users.

REFERENCES

Source Control: PL-04
Supporting Publications: SP 800-18 [63]

3.16. System and Services Acquisition

3.16.1. Acquisition Process

REQUIREMENT: 03.16.01

Include the following security requirements, explicitly or by reference, in the acquisition contract for the system, system component, or system service: [*Assignment: organization-defined security requirements*].

DISCUSSION

Security requirements include security functional and security assurance requirements. Security functional requirements are typically derived from mission or business requirements as well as requirements stated in laws, regulations, policies, and standards. The derived requirements can include security capabilities, functions, and mechanisms. Assurance requirements can include development processes, procedures, methodologies, and the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. Strength of mechanism requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. This requirement is related to 03.16.03 and 03.17.02.

REFERENCES

Source Control: SA-04
Supporting Publications: SP 800-160-1 [11], SP 800-160-2 [10], SP 800-161 [33]

3.16.2. Unsupported System Components

REQUIREMENT: 03.16.02

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

b. Provide options for risk mitigation or alternative sources for continued support for unsupported components if components cannot be replaced.

DISCUSSION

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in opportunities for adversaries to exploit weaknesses or deficiencies in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities when newer technologies are unavailable or when the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

REFERENCES

Source Control: SA-22
Supporting Publications: None

3.16.3. External System Services

REQUIREMENT: 03.16.03

a. Require the providers of external system services used for the processing, storage, or transmission of CUI, to comply with the following security requirements: [*Assignment: organization-defined security requirements*].

b. Define and document user roles and responsibilities with regard to external system services including shared responsibilities with external providers.

c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

DISCUSSION

External system services are provided by external service providers. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with the organization charged with protecting

CUI. Service-level agreements define the expectations of performance, describe measurable outcomes, and identify remedies, mitigations, and response requirements for instances of noncompliance. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when there is a need to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols. This requirement is related to 03.01.20.

REFERENCES

Source Control: SA-09
Supporting Publications: SP 800-160-1 [11], SP 800-161 [33]

3.17. Supply Chain Risk Management

3.17.1. Supply Chain Risk Management Plan

REQUIREMENT: 03.17.01

a. Develop a plan for managing supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.

b. Review and update the supply chain risk management plan periodically.

c. Protect the supply chain risk management plan from unauthorized disclosure.

DISCUSSION

Dependence on the products, systems, and services from external providers and the nature of the relationships with those providers present an increasing level of risk to an organization. Threat actions that may increase security risks include unauthorized production; the insertion or use of counterfeits; tampering; theft; the insertion of malicious software, firmware, and hardware; and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system, component, or service. Managing supply chain risks is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.

Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against the plans. The system-level SCRM plan is implementation-specific and provides policy implementation, requirements, constraints, and implications. It can either be stand-alone or incorporated into system security plans. The SCRM plan addresses the management, implementation, and monitoring of SCRM controls and the development or sustainment of systems across the system development life cycle to support mission and business functions. Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to individual program, organizational, and operational contexts.

REFERENCES

Source Control: SR-02
Supporting Publications: SP 800-30 [55], SP 800-39 [60], SP 800-160-1 [11], SP 800-181 [34]

3.17.2. Acquisition Strategies, Tools, and Methods

REQUIREMENT: 03.17.02

Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

DISCUSSION

The acquisition process provides an important vehicle for protecting the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, the insertion of counterfeits, the insertion of malicious software or backdoors, and poor development practices throughout the system life cycle.

Organizations also consider providing incentives for suppliers to implement controls, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security requirements of the organization. Contracts may specify documentation protection requirements.

REFERENCES

Source Control: SR-05
Supporting Publications: SP 800-30 [55], SP 800-161 [33]

3.17.3. Supply Chain Requirements and Processes

REQUIREMENT: 03.17.03

a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.

b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [*Assignment: organization-defined security requirements*].

DISCUSSION

Supply chain elements include organizations, entities, or tools that are employed for the research, development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, firmware, and systems development processes; shipping and handling procedures; personnel and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance, and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or

processes represent potential vulnerabilities that can be exploited by adversaries to harm the organization and affect its ability to carry out its core missions or business functions.

REFERENCES

Source Control: SR-03
Supporting Publications: SP 800-30 [55], SP 800-161 [33]

References

[1] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010. Available at https://www.govinfo.gov/app/details/DCPD-201000942

[2] Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009. Available at https://www.govinfo.gov/app/details/DCPD-200901022

[3] Atomic Energy Act (P.L. 83-703), August 1954. Available at https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919

[4] National Archives and Records Administration (2019) Controlled Unclassified Information (CUI) Registry. Available at https://www.archives.gov/cui

[5] 32 CFR Part 2002 (2016), Controlled Unclassified Information (CUI), September 2016. Available at https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf

[6] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[7] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[8] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[9] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[10] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[11] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[12] Joint Task Force (2020) Control Baselines for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[13] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[14] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2

[15] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[16] Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1

[17] Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1

[18] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1

[19] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[20] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[21] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-121, Rev. 2, Includes updates as of January 19, 2022. https://doi.org/10.6028/NIST.SP.800-121r2-upd1

[22] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[23] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-178. https://doi.org/10.6028/NIST.SP.800-178

[24] Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-192. https://doi.org/10.6028/NIST.SP.800-192

[25] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[26] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and Automated Access Management Using Secure Shell (SSH). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966. https://doi.org/10.6028/NIST.IR.7966

[27] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[28] Howell G, Franklin JM, Sritapan V, Souppaya M, Scarfone K (2023) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 2. https://doi.org/10.6028/NIST.SP.800-124r2

[29] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[30] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97

[31] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[32] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[33] Boyens JM, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161, Rev. 1. https://doi.org/10.6028/NIST.SP.800-161r1

[34] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[35] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[36] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86

[37] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1

[38] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[39] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[40] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

[41] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[42] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2

[43] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Volume 3: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3

[44] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4

[45] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3

[46] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167

[47] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[48] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

[49] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[50] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[51] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111

[52] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[53] Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800-130

[54] Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-152. https://doi.org/10.6028/NIST.SP.800-152

[55] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[56] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4

[57] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[58] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[59] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[60] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[61] Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1. https://doi.org/10.6028/NIST.SP.800-12r1

[62] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[63] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[64] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1

[65] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B

[66] Rose S, Borchert O, Mitchell S, Connelly S (2017) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[67] Sriram K, Montgomery D (2019) Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-189. https://doi.org/10.6028/NIST.SP.800-189

[68] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 197, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

[69] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2

[70] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-177, Rev. 1. https://doi.org/10.6028/NIST.SP.800-177r1

[71] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2

[72] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95

[73] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[74] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2

[75] Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Cr2

[76] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1

[77] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2

[78] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[79] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552

[80] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331

[81] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35-subchapI-sec3502

[82] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-81-2. https://doi.org/10.6028/NIST.SP.800-81-2

[83] Dempsey K, Pillitteri V, Regenscheid A (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1

Appendix A. Acronyms

CFR
Code of Federal Regulations

CISA
Cybersecurity and Infrastructure Security Agency

CUI
Controlled Unclassified Information

CVE
Common Vulnerabilities and Exposures

CVSS
Common Vulnerabilities Scoring System

CWE
Common Weakness Enumeration

DMZ
Demilitarized Zone

EAP
Extensible Authentication Protocol

EO
Executive Order

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

FTP
File Transfer Protocol

GMT
Greenwich Mean Time

IEEE
Institute of Electrical and Electronics Engineers

IIoT
Industrial Internet of Things

IoT
Internet of Things

ISOO
Information Security Oversight Office

IT
Information Technology

LSI
Large-Scale Integration

MAC
Media Access Control

NARA
National Archives and Records Administration

NVD
National Vulnerabilities Database

ODP
Organization-Defined Parameter

OMB
Office of Management and Budget

OT
Operational Technology

PII
Personally Identifiable Information

PIN
Personal Identification Number

PROM
Programmable Read-Only Memory

ROM
Read-Only Memory

SCAP
Security Content Automation Protocol

SCRM
Supply Chain Risk Management

SP
Special Publication

TCP/IP
Transmission Control Protocol/Internet Protocol

TLS
Transport Layer Security

UTC
Coordinated Universal Time

Appendix B. Glossary

Appendix B provides definitions for the terminology used in NIST SP 800-171. The definitions are consistent with the definitions contained in the National Information Assurance Glossary [78] unless otherwise noted.

agency
Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. [13]

assessment
See *security control assessment*.

assessor
See *security control assessor*.

audit log
A chronological record of system activities, including records of system accesses and operations performed in a given period.

audit record
An individual entry in an audit log related to an audited event.

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. Adapted from [7].

availability
Ensuring timely and reliable access to and use of information. [79]

advanced persistent threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives. [60]

authenticator
Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was previously referred to as a token.

baseline configuration
A documented set of specifications for a system or a configuration item within a system that has been formally reviewed and agreed upon at a given point in time, and that can only be changed through change control procedures.

common secure configuration
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. These benchmarks are also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides.

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [79]

configuration management
A collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

configuration settings
The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.

controlled area
Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

controlled unclassified information
Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [1]

CUI Executive Agent
The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO). [5]

CUI program
The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry. [5]

CUI registry
The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. [5]

cyber-physical systems
Interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

executive agency
An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.

external system (or component)
A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

external system service
A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by but not a part of the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

external network
A network not controlled by the organization.

facility
One or more physical locations containing systems or system components that process, store, or transmit information.

federal agency
See *executive agency*.

federal information system
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [80]

FIPS-validated cryptography
A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet the requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-approved cryptography*.

firmware
Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software*. [78]

hardware
The material physical components of a system. See *software* and *firmware*. [78]

identifier
Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

A unique label used by a system to indicate a specific entity, object, or group.

impact
With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

impact value
The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high. [6]

incident
An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [79]

information
Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [13]

information flow control
Procedure to ensure that information transfers within a system do not violate the security policy.

information resources
Information and related resources, such as personnel, equipment, funds, and information technology. [81]

information security
The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [79]

information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [81]

information technology
Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. [13]

insider threat
The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

integrity
Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [79]

internal network
A network in which the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors or in which the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.

least privilege
The principle that a security architecture is designed so that each entity is granted the minimum system authorizations and resources needed to perform its function.

malicious code
Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system. Examples of malicious code include viruses, worms, Trojan horses, spyware, some forms of adware, or other code-based entities that infect a host.

media
Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system. [7]

mobile code
Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

mobile device
A portable 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 devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and e-readers.

multi-factor authentication
Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric). See *authenticator*.

network
A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access
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, the internet).

nonfederal organization
An entity that owns, operates, or maintains a nonfederal system.

nonfederal system
A system that does not meet the criteria for a federal system.

nonlocal maintenance
Maintenance activities conducted by individuals communicating through an external network (e.g., the internet) or an internal network.

NSA-approved cryptography
Cryptography that consists of an approved algorithm, an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a specific environment, and a supporting key management infrastructure. [8]

on behalf of (an agency)
A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government. [5]

organization
An entity of any size, complexity, or positioning within an organizational structure. Adapted from [7]

organization-defined parameter
The variable part of a security requirement that is instantiated by an organization during the tailoring process by assigning an organization-defined value as part of the requirement. Adapted from [8].

overlay
A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. [13]

personnel security
The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness. [8]

portable storage device
A system component that can be inserted into and removed from a system and that is used to store information or data (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, flash memory cards/drives that contain nonvolatile memory).

potential impact
The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals. [6]

privileged account
A system account with the authorizations of a privileged user.

privileged user
A user who is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

records
The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results) that serve as a basis for verifying that the organization and the system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain a complete set of information on particular items).

remote access
Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the internet). Remote access methods include dial-up, broadband, and wireless.

remote maintenance
Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).

replay resistant
Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [13]

risk assessment
The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. [55]

sanitization
Actions taken to render data written on media unrecoverable by ordinary and — for some forms of sanitization — extraordinary means.

A process to remove information from media such that data recovery is not possible, including the removal of all classified labels, markings, and activity logs.

security
A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. [78]

security assessment
See *security control assessment*.

security control
The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [13]

security control assessment
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [13]

security domain
A domain that implements a security policy and is administered by a single authority. Adapted from [78]

security functions
The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

security requirement
A requirement levied on a system or an organization that is derived from applicable laws, Executive Orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Adapted from [7] and [8].

split tunneling
The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.

system
See *information system*.

system component
A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware. [41]

system security plan
A document that describes how an organization meets or plans to meet the security requirements for a system. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems.

system service
A capability provided by a system that facilitates information processing, storage, or transmission.

threat
Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [55]

system user
An individual or (system) process acting on behalf of an individual that is authorized to access a system.

Appendix C. Tailoring Criteria

This appendix describes the security control tailoring criteria used to develop the CUI security requirements. Table 2 lists the available tailoring options and the shorthand tailoring symbols. Table 3 through Table 22 specify the tailoring actions applied to the controls in the NIST SP 800-53 moderate baseline [12] to obtain the security requirements in Section 3. The controls and control enhancements are hyperlinked to the NIST Cybersecurity and Privacy Reference Tool, which provides online access to the specific control language and supplemental materials in NIST SP 800-53.

Table 2. Security control tailoring criteria

TAILORING SYMBOL	TAILORING CRITERIA
NCO	The control is not directly related to protecting the confidentiality of CUI.
FED	The control is primarily the responsibility of the Federal Government.
ORC	The outcome of the control relating to the protection of confidentiality of CUI is adequately covered by other related controls.[16]
N/A	The control is not applicable.
CUI	The control is directly related to protecting the confidentiality of CUI.

Table 3. Access Control (AC)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AC-01	Policy and Procedures	CUI	03.15.01
AC-02	Account Management	CUI	03.01.01
AC-02(01)	Account Management | Automated System Account Management	NCO	—
AC-02(02)	Account Management | Automated Temporary and Emergency Account Management	NCO	—
AC-02(03)	Account Management | Disable Accounts	CUI	03.01.01
AC-02(04)	Account Management | Automated Audit Actions	NCO	—
AC-02(05)	Account Management | Inactivity Logout	ORC	—
AC-02(13)	Account Management | Disable Accounts for High-Risk Individuals	CUI	03.01.01
AC-03	Access Enforcement	CUI	03.01.02
AC-04	Information Flow Enforcement	CUI	03.01.03
AC-05	Separation of Duties	CUI	03.01.04
AC-06	Least Privilege	CUI	03.01.05
AC-06(01)	Least Privilege | Authorize Access to Security Functions	CUI	03.01.05
AC-06(02)	Least Privilege | Non-Privileged Access for Nonsecurity Functions	CUI	03.01.06
AC-06(05)	Least Privilege | Privileged Accounts	CUI	03.01.06
AC-06(07)	Least Privilege | Review of User Privileges	CUI	03.01.05

[16] The security controls in NIST SP 800-53 provide a comprehensive set of security capabilities needed to protect organizational systems that taken together, support the concept of defense-in-depth. As such, some of the security controls may address similar or overlapping security topics that are covered by other related controls. These controls have been designated as ORC in the tailoring criteria.

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AC-06(09)	Least Privilege | Log Use of Privileged Functions	CUI	03.01.07
AC-06(10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	CUI	03.01.07
AC-07	Unsuccessful Logon Attempts	CUI	03.01.08
AC-08	System Use Notification	CUI	03.01.09
AC-11	Device Lock	CUI	03.01.10
AC-11(01)	Device Lock | Pattern-Hiding Displays	CUI	03.01.10
AC-12	Session Termination	CUI	03.01.11
AC-14	Permitted Actions Without Identification or Authentication	FED	—
AC-17	Remote Access	CUI	03.01.02
AC-17(01)	Remote Access | Monitoring and Control	NCO	—
AC-17(02)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	CUI	03.13.08
AC-17(03)	Remote Access | Managed Access Control Points	CUI	03.01.12
AC-17(04)	Remote Access | Privileged Commands and Access	CUI	03.01.12
AC-18	Wireless Access	CUI	03.01.16
AC-18(01)	Wireless Access | Authentication and Encryption	ORC	—
AC-18(03)	Wireless Access | Disable Wireless Networking	CUI	03.01.16
AC-19	Access Control for Mobile Devices	CUI	03.01.18
AC-19(05)	Access Control for Mobile Devices | Full Device or Container-Based Encryption	CUI	03.01.18
AC-20	Use of External Systems	CUI	03.01.20
AC-20(01)	Use of External Systems | Limits on Authorized Use	CUI	03.01.20
AC-20(02)	Use of External Systems | Portable Storage Devices – Restricted Use	CUI	03.01.20
AC-21	Information Sharing	FED	—
AC-22	Publicly Accessible Content	CUI	03.01.22

Table 4. Awareness and Training (AT)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AT-01	Policy and Procedures	CUI	03.15.01
AT-02	Literacy Training and Awareness	CUI	03.02.01
AT-02(02)	Literacy Training and Awareness | Insider Threat	CUI	03.02.01
AT-02(03)	Literacy Training and Awareness | Social Engineering and Mining	CUI	03.02.01
AT-03	Role-Based Training	CUI	03.02.02
AT-04	Training Records	NCO	—

Table 5. Audit and Accountability (AU)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AU-01	Policy and Procedures	CUI	03.15.01

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AU-02	Event Logging	CUI	03.03.01
AU-03	Content of Audit Records	CUI	03.03.02
AU-03(01)	Additional Audit Information	CUI	03.03.02
AU-04	Audit Log Storage Capacity	NCO	—
AU-05	Response to Audit Logging Process Failures	CUI	03.03.04
AU-06	Audit Record Review, Analysis, and Reporting	CUI	03.03.05
AU-06(01)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	NCO	—
AU-06(03)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	CUI	03.03.05
AU-07	Audit Record Reduction and Report Generation	CUI	03.03.06
AU-07(01)	Audit Record Reduction and Report Generation | Automatic Processing	NCO	—
AU-08	Time Stamps	CUI	03.03.07
AU-09	Protection of Audit Information	CUI	03.03.08
AU-09(04)	Protection of Audit Information | Access by Subset of Privileged Users	CUI	03.03.08
AU-11	Audit Record Retention	CUI	03.03.03
AU-12	Audit Record Generation	CUI	03.03.03

Table 6. Assessment, Authorization, and Monitoring (CA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CA-01	Policy and Procedures	CUI	03.15.01
CA-02	Control Assessments	CUI	03.12.01
CA-02(01)	Control Assessments | Independent Assessors	NCO	—
CA-03	Information Exchange	CUI	03.12.05
CA-05	Plan of Action and Milestones	CUI	03.12.02
CA-06	Authorization	FED	—
CA-07	Continuous Monitoring	CUI	03.12.03
CA-07(01)	Continuous Monitoring | Independent Assessment	NCO	—
CA-07(04)	Continuous Monitoring | Risk Monitoring	NCO	—
CA-09	Internal System Connections	NCO	—

Table 7. Configuration Management (CM)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CM-01	Policy and Procedures	CUI	03.15.01
CM-02	Baseline Configuration	CUI	03.04.01
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency	NCO	—
CM-02(03)	Baseline Configuration | Retention of Previous Configurations	NCO	—
CM-02(07)	Baseline Configuration | Configure Systems and Components for High-Risk Areas	CUI	03.04.12

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CM-03	Configuration Change Control	CUI	03.04.03
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	NCO	—
CM-03(04)	Configuration Change Control | Security and Privacy Representatives	NCO	—
CM-04	Impact Analyses	CUI	03.04.04
CM-04(02)	Impact Analyses | Verification of Controls	ORC	—
CM-05	Access Restrictions for Change	CUI	03.04.05
CM-06	Configuration Settings	CUI	03.04.02
CM-07	Least Functionality	CUI	03.04.06
CM-07(01)	Least Functionality | Periodic Review	CUI	03.04.06
CM-07(02)	Least Functionality | Prevent Program Execution	ORC	—
CM-07(05)	Least Functionality | Authorized Software – Allow by Exception	CUI	03.04.08
CM-08	System Component Inventory	CUI	03.04.10
CM-08(01)	System Component Inventory | Updates During Installation and Removal	CUI	03.04.10
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	NCO	—
CM-09	Configuration Management Plan	NCO	—
CM-10	Software Usage Restrictions	NCO	—
CM-11	User-Installed Software	ORC	—
CM-12	Information Location	CUI	03.04.11
CM-12(01)	Information Location | Automated Tools to Support Information Location	NCO	—

Table 8. Contingency Planning (CP)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CP-01	Policy and Procedures	NCO	—
CP-02	Contingency Plan	NCO	—
CP-02(01)	Contingency Plan | Coordinate with Related Plans	NCO	—
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	NCO	—
CP-02(08)	Contingency Plan | Identify Critical Assets	NCO	—
CP-03	Contingency Training	NCO	—
CP-04	Contingency Plan Testing	NCO	—
CP-04(01)	Contingency Plan Testing | Coordinate Related Plans	NCO	—
CP-06	Alternate Storage Site	NCO	—
CP-06(01)	Alternate Storage Site | Separation of Primary Site	NCO	—
CP-06(03)	Alternate Storage Site | Accessibility	NCO	—
CP-07	Alternate Processing Site	NCO	—
CP-07(01)	Alternate Processing Site | Separation of Primary Site	NCO	—
CP-07(02)	Alternate Processing Site | Accessibility	NCO	—
CP-07(03)	Alternate Processing Site | Priority of Service	NCO	—
CP-08	Telecommunications Services	NCO	—

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CP-08(01)	Telecommunications Services | Priority of Service Provisions	NCO	—
CP-08(02)	Telecommunications Services | Single Points of Failure	NCO	—
CP-09	System Backup	NCO	—
CP-09(01)	System Backup | Testing for Reliability and Integrity	NCO	—
CP-09(08)	System Backup | Cryptographic Protection	CUI	03.08.09
CP-10	System Recovery and Reconstitution	NCO	—
CP-10(02)	System Recovery and Reconstitution | Transaction Recovery	NCO	—

2904 **Table 9.** Identification and Authentication (IA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IA-01	Policy and Procedures	CUI	03.15.01
IA-02	Identification and Authentication (Organizational Users)	CUI	03.05.01
IA-02(01)	Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts	CUI	03.05.03
IA-02(02)	Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts	CUI	03.05.03
IA-02(08)	Identification and Authentication (Organizational Users) | Access to Accounts – Replay Resistant	CUI	03.05.04
IA-02(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	FED	—
IA-03	Device Identification and Authentication	CUI	03.05.02
IA-04	Identifier Management	CUI	03.05.05
IA-04(04)	Identifier Management | Identify User Status	CUI	03.05.05
IA-05	Authenticator Management	CUI	03.05.12
IA-05(01)	Authenticator Management | Password-Based Authentication	CUI	03.05.07
IA-05(02)	Authenticator Management | Public Key-Based Authentication	FED	—
IA-05(06)	Authenticator Management | Protection of Authenticators	ORC	—
IA-06	Authentication Feedback	CUI	03.05.11
IA-07	Cryptographic Module Authentication	FED	—
IA-08	Identification and Authentication (Non-Organizational Users)	FED	—
IA-08(01)	Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies	FED	—
IA-08(02)	Identification and Authentication (Non-Organizational Users) | Acceptance of External Authenticators	FED	—
IA-08(04)	Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles	FED	—
IA-11	Re-Authentication	CUI	03.05.01
IA-12	Identity Proofing	FED	—
IA-12(02)	Identity Proofing | Identity Evidence	FED	—
IA-12(03)	Identity Proofing | Identity Evidence Validation and Verification	FED	—
IA-12(05)	Identity Proofing | Address Confirmation	FED	—

2905

2906

2907 **Table 10.** Incident Response (IR)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IR-01	Policy and Procedures	CUI	03.15.01
IR-02	Incident Response Training	CUI	03.06.04
IR-03	Incident Response Testing	CUI	03.06.03
IR-03(02)	Incident Response Testing | Coordinate with Related Plans	NCO	—
IR-04	Incident Handling	CUI	03.06.01
IR-04(01)	Incident Handling | Automated Incident Handling Processes	NCO	—
IR-05	Incident Monitoring	CUI	03.06.02
IR-06	Incident Reporting	CUI	03.06.02
IR-06(01)	Incident Reporting | Automated Reporting	NCO	—
IR-06(03)	Incident Reporting | Supply Chain Coordination	NCO	—
IR-07	Incident Response Assistance	CUI	03.06.02
IR-07(01)	Incident Response Assistance | Automation Support for Availability of Information and Support	NCO	—
IR-08	Incident Response Plan	CUI	03.06.01

2908

2909 **Table 11.** Maintenance (MA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MA-01	System Maintenance Policy and Procedures	CUI	03.15.01
MA-02	Controlled Maintenance	NCO	—
MA-03	Maintenance Tools	CUI	03.07.04
MA-03(01)	Maintenance Tools | Inspect Tools	CUI	03.07.04
MA-03(02)	Maintenance Tools | Inspect Media	CUI	03.07.04
MA-03(03)	Maintenance Tools | Prevent Unauthorized Removal	CUI	03.07.04
MA-04	Nonlocal Maintenance	CUI	03.07.05
MA-04(02)	Nonlocal Maintenance | Document Nonlocal Maintenance	NCO	—
MA-05	Maintenance Personnel	CUI	03.07.06
MA-06	Timely Maintenance	NCO	—

2910

2911 **Table 12.** Media Protection (MP)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MP-01	Policy and Procedures	CUI	03.15.01
MP-02	Media Access	CUI	03.08.02
MP-03	Media Marking	CUI	03.08.04
MP-04	Media Storage	CUI	03.08.01
MP-05	Media Transport	CUI	03.08.05
MP-06	Media Sanitization	CUI	03.08.03
MP-07	Media Use	CUI	03.08.07

2912 **Table 13.** Physical and Environmental Protection (PE)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PE-01	Policy and Procedures	CUI	03.15.01
PE-02	Physical Access Authorizations	CUI	03.10.01
PE-03	Physical Access Control	CUI	03.10.07
PE-04	Access Control for Transmission	CUI	03.10.08
PE-05	Access Control for Output Devices	CUI	03.10.08
PE-06	Monitoring Physical Access	CUI	03.10.02
PE-06(01)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	NCO	—
PE-08	Visitor Access Records	NCO	—
PE-09	Power Equipment and Cabling	NCO	—
PE-10	Emergency Shutoff	NCO	—
PE-11	Emergency Power	NCO	—
PE-12	Emergency Lighting	NCO	—
PE-13	Fire Protection	NCO	—
PE-13(01)	Fire Protection | Detection Systems – Automatic Activation and Notification	NCO	—
PE-14	Environmental Controls	NCO	—
PE-15	Water Damage Protection	NCO	—
PE-16	Delivery and Removal	NCO	—
PE-17	Alternate Work Site	CUI	03.10.06

2913

2914 **Table 14.** Planning (PL)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PL-01	Policy and Procedures	CUI	03.15.01
PL-02	System Security and Privacy Plans	CUI	03.15.02
PL-04	Rules of Behavior	CUI	03.15.03
PL-04(01)	Rules of Behavior | Social Media and External Site/Application Usage Restrictions	NCO	—
PL-08	Security and Privacy Architectures	NCO	—
PL-10	Baseline Selection	FED	—
PL-11	Baseline Tailoring	FED	—

2915

2916 **Table 15.** Program Management (PM)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PM-01	Information Security Program Plan	N/A	—
PM-02	Information Security Program Leadership Role	N/A	—
PM-03	Information Security and Privacy Resources	N/A	—

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PM-04	Plan of Action and Milestones Process	N/A	—
PM-05	System Inventory	N/A	—
PM-05(01)	System Inventory | Inventory of Personally Identifiable Information	N/A	—
PM-06	Measures of Performance	N/A	—
PM-07	Enterprise Architecture	N/A	—
PM-07(01)	Enterprise Architecture | Offloading	N/A	—
PM-08	Critical Infrastructure Plan	N/A	—
PM-09	Risk Management Strategy	N/A	—
PM-10	Authorization Process	N/A	—
PM-11	Mission and Business Process Definition	N/A	—
PM-12	Insider Threat Program	N/A	—
PM-13	Security and Privacy Workforce	N/A	—
PM-14	Testing, Training, and Monitoring	N/A	—
PM-15	Security and Privacy Groups and Associations	N/A	—
PM-16	Threat Awareness Program	N/A	—
PM-16(01)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	N/A	—
PM-17	Protecting Controlled Unclassified Information on External Systems	N/A	—
PM-18	Privacy Program Plan	N/A	—
PM-19	Privacy Program Leadership Role	N/A	—
PM-20	Dissemination of Privacy Program Information	N/A	—
PM-20(01)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	N/A	—
PM-21	Accounting of Disclosures	N/A	—
PM-22	Personally Identifiable Information Quality Management	N/A	—
PM-23	Data Governance Body	N/A	—
PM-24	Data Integrity Board	N/A	—
PM-25	Minimization of PII Used in Testing, Training, and Research	N/A	—
PM-26	Complaint Management	N/A	—
PM-27	Privacy Reporting	N/A	—
PM-28	Risk Framing	N/A	—
PM-29	Risk Management Program Leadership Roles	N/A	—
PM-30	Supply Chain Risk Management Strategy	N/A	—
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-Essential Items	N/A	—
PM-31	Continuous Monitoring Strategy	N/A	—
PM-32	Purposing	N/A	—

Table 16. Personnel Security (PS)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PS-01	Policy and Procedures	CUI	03.15.01
PS-02	Position Risk Designation	FED	—

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PS-03	Personnel Screening	CUI	03.09.01
PS-04	Personnel Termination	CUI	03.09.02
PS-05	Personnel Transfer	CUI	03.09.02
PS-06	Access Agreements	ORC	—
PS-07	External Personnel Security	ORC	—
PS-08	Personnel Sanctions	NCO	—
PS-09	Position Descriptions	FED	—

Table 17. PII Processing and Transparency (PT)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PT-01	Policy and Procedures	N/A	—
PT-02	Authority to Process Personally Identifiable Information	N/A	—
PT-02(01)	Authority to Process Personally Identifiable Information | Data Tagging	N/A	—
PT-02(02)	Authority to Process Personally Identifiable Information | Automation	N/A	—
PT-03	Personally Identifiable Information Processing Purposes	N/A	—
PT-03(01)	Personally Identifiable Information Processing Purposes | Data Tagging	N/A	—
PT-03(02)	Personally Identifiable Information Processing Purposes | Automation	N/A	—
PT-04	Consent	N/A	—
PT-04(01)	Consent | Tailored Consent	N/A	—
PT-04(02)	Consent | Just-in-Time Consent	N/A	—
PT-04(03)	Consent | Revocation	N/A	—
PT-05	Privacy Notice	N/A	—
PT-05(01)	Privacy Notice | Just-in-Time Notice	N/A	—
PT-05(02)	Privacy Notice | Privacy Act Statements	N/A	—
PT-06	System of Records Notice	N/A	—
PT-06(01)	System of Records Notice | Routine Uses	N/A	—
PT-06(02)	System of Records Notice | Exemption Rules	N/A	—
PT-07	Specific Categories of Personally Identifiable Information	N/A	—
PT-07(01)	Specific Categories of Personally Identifiable Information | Social Security Numbers	N/A	—
PT-07(02)	Specific Categories of Personally Identifiable Information | First Amendment Information	N/A	—
PT-08	Computer Matching Requirements	N/A	—

Table 18. Risk Assessment (RA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
RA-01	Policy and Procedures	CUI	03.15.01
RA-02	Security Categorization	FED	—

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
RA-03	Risk Assessment	CUI	03.11.01
RA-03(01)	Risk Assessment | Supply Chain Risk Assessment	CUI	03.11.01
RA-05	Vulnerability Monitoring and Scanning	CUI	03.11.02
RA-05(02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned	CUI	03.11.02
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access	ORC	—
RA-05(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	NCO	—
RA-07	Risk Response	ORC	—
RA-09	Criticality Analysis	NCO	—

Table 19. System and Services Acquisition (SA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SA-01	Policy and Procedures	CUI	03.15.01
SA-02	Allocation of Resources	NCO	—
SA-03	System Development Life Cycle	NCO	—
SA-04	Acquisition Process	CUI	03.16.01
SA-04(01)	Acquisition Process | Functional Properties of Controls	NCO	—
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	NCO	—
SA-04(09)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	NCO	—
SA-04(10)	Acquisition Process | Use of Approved PIV Products	FED	—
SA-05	System Documentation	NCO	—
SA-08	Security and Privacy Engineering Principles	NCO	—
SA-09	External System Services	CUI	03.16.03
SA-09(02)	External System Services | Identification of Functions, Ports, Protocols, and Services	NCO	—
SA-10	Developer Configuration Management	ORC	—
SA-11	Developer Testing and Evaluation	ORC	—
SA-15	Development Process, Standards, and Tools	ORC	—
SA-15(03)	Development Process, Standards, and Tools | Criticality Analysis	NCO	—
SA-22	Unsupported System Components	CUI	03.16.02

Table 20. System and Communications Protection (SC)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SC-01	Policy and Procedures	CUI	03.15.01
SC-02	Separation of System and User Functionality	ORC	—
SC-04	Information in Shared System Resources	CUI	03.13.04
SC-05	Denial-of-Service Protection	NCO	—
SC-07	Boundary Protection	CUI	03.13.01

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SC-07(03)	Boundary Protection | Access Points	ORC	—
SC-07(04)	Boundary Protection | External Telecommunications Services	ORC	—
SC-07(05)	Boundary Protection | Deny by Default – Allow by Exception	CUI	03.13.06
SC-07(07)	Boundary Protection | Split Tunneling for Remote Devices	ORC	—
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	ORC	—
SC-08	Transmission Confidentiality and Integrity	CUI	03.13.08
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	CUI	03.13.08
SC-10	Network Disconnect	CUI	03.13.09
SC-12	Cryptographic Key Establishment and Management	CUI	03.13.10
SC-13	Cryptographic Protection	CUI	03.13.11
SC-15	Collaborative Computing Devices and Applications	CUI	03.13.12
SC-17	Public Key Infrastructure Certificates	FED	—
SC-18	Mobile Code	CUI	03.13.13
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	NCO	—
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NCO	—
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NCO	—
SC-23	Session Authenticity	CUI	03.13.15
SC-28	Protection of Information at Rest	CUI	03.13.08
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	CUI	03.13.08
SC-39	Process Isolation	NCO	—

Table 21. System and Information Integrity (SI)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SI-01	Policy and Procedures	CUI	03.15.01
SI-02	Flaw Remediation	CUI	03.14.01
SI-02(02)	Flaw Remediation | Automated Flaw Remediation Status	NCO	—
SI-03	Malicious Code Protection	CUI	03.14.02
SI-04	System Monitoring	CUI	03.14.06
SI-04(02)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	NCO	—
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic	CUI	03.14.06
SI-04(05)	System Monitoring | System-Generated Alerts	NCO	—
SI-05	Security Alerts, Advisories, and Directives	CUI	03.14.03
SI-07	Software, Firmware, and Information Integrity	NCO	—
SI-07(01)	Software, Firmware, and Information Integrity | Integrity Checks	NCO	—
SI-07(07)	Software, Firmware, and Information Integrity | Integration of Detection and Response	NCO	—
SI-08	Spam Protection	ORC	—
SI-08(02)	Spam Protection | Automatic Updates	NCO	—
SI-10	Information Input Validation	NCO	—
SI-11	Error Handling	NCO	—

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SI-12	Information Management and Retention	CUI	03.14.08
SI-16	Memory Protection	NCO	—

Table 22. Supply Chain Risk Management (SR)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SR-01	Policy and Procedures	CUI	03.15.01
SR-02	Supply Chain Risk Management Plan	CUI	03.17.01
SR-02(01)	Supply Chain Risk Management Plan | Establish SCRM Team	NCO	—
SR-03	Supply Chain Controls and Processes	CUI	03.17.03
SR-05	Acquisition Strategies, Tools, and Methods	CUI	03.17.02
SR-06	Supplier Assessments and Reviews	CUI	03.11.01
SR-08	Notification Agreements	NCO	—
SR-10	Inspection of Systems or Components	NCO	—
SR-11	Component Authenticity	NCO	—
SR-11(01)	Component Authenticity | Anti-Counterfeit Training	NCO	—
SR-11(02)	Component Authenticity | Configuration Control for Component Service and Repair	NCO	—
SR-12	Component Disposal	ORC	—

Appendix D. Change Log

This publication incorporates the following changes from the original edition (February 2020; updated January 28, 2021):

- Streamlined introductory information in Section 1 and Section 2 to improve clarity and understanding
- Modified the security requirements and families in Section 3 to reflect the security controls in the NIST SP 800-53B [12] moderate baseline and the tailoring actions in Appendix C
- Eliminated the distinction between basic and derived security requirements
- Increased the specificity of security requirements to remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments
- Introduced organization-defined parameters (ODPs) in selected security requirements to increase flexibility and help organizations better manage risk
- Grouped security requirements, where possible, to improve understanding and the efficiency of implementations and assessments
- Removed outdated and redundant security requirements
- Added new security requirements
- Added titles to security requirements
- Restructured and streamlined the discussion sections for security requirements
- Introduced new tailoring categories: *Other Related Controls (ORC)* and *Not Applicable (N/A)*
- Recategorized selected controls in the NIST SP 800-53B moderate baseline (using the tailoring criteria in Appendix C)
- Revised the security requirements for consistency with the security control language in NIST SP 800-53
- Revised the structure of the References, Acronyms, and Glossary sections for greater clarity and ease of use
- Revised the tailoring tables in Appendix C for consistency with the changes to the security requirements

Table 23 shows the changes incorporated into this publication. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates to this document that are not yet published in an errata update or a formal revision, including additional issues and potential corrections, will be posted as they are identified. See the publication details for this report. The current release of this publication does not include any errata updates.

Table 23. Change Log

Publication ID	Date	Type of Edit	Change	Location