NIST Special Publication
NIST SP 800-171r3 ipd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Initial Public Draft

Ron Ross
Victoria Pillitteri

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

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

NIST Special Publication
NIST SP 800-171r3 ipd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Initial 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.ipd

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

Author ORCID iDs

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

Public Comment Period

May 10, 2023 – July 14, 2023

Contact Information

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 agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations, when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency, and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. 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

basic security requirement; contractor systems; Controlled Unclassified Information; CUI Registry; derived security requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; nonfederal organizations; nonfederal systems; 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 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)
- Acquisition or procurement responsibilities (e.g., contracting officers)
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts)

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 represents over one year of data collection, technical analysis, customer interaction, redesign, and development of the security requirements and supporting information for the protection of Controlled Unclassified Information (CUI). Many trade-offs have been made to ensure that the technical and non-technical requirements have been stated clearly and concisely, while at the same time recognizing the specific needs of both federal and nonfederal organizations. The following provides a summary of the significant changes that have been made to NIST SP 800-171 in transitioning from Revision 2 to Revision 3:

- Streamlined introductory information in Section 1 and Section 2 to improve clarity and customer understanding
- Modified the security requirements and families in Section 3 to reflect the controls in the NIST SP 800-53B [13] 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 (ODP) in selected security requirements to increase flexibility and help organizations better manage risk
- Grouped security requirements, where possible, to improve understanding and efficiency of implementation and assessments
- Removed outdated and redundant security requirements
- Added titles to security requirements
- Introduced a new tailoring category, *Not Applicable (NA)*
- Recategorized selected controls in the NIST SP 800-53B moderate baseline (using the tailoring criteria in Appendix C)
- Recast the security requirements, where possible, for consistency with the security control language in NIST SP 800-53
- Developed a prototype CUI overlay that expresses security requirements using the tailored security controls 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 table in Appendix C for consistency with the changes to the security requirements
- Transitioned the mapping tables formerly resident in Appendix D of NIST SP 800-171, Revision 2 to the publication details web page along with other supporting material

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.

NIST is specifically interested in comments, feedback, and recommendations for the following topics:

- Re-categorized controls (e.g., controls formerly categorized as NFO)
- Inclusion of organization-defined parameters (ODP)
- Prototype CUI overlay

Reviewers are encouraged to comment on all or parts of draft NIST SP 800-171, Revision 3. NIST requests that all comments be submitted to 800-171comments@list.nist.gov by 11:59 PM Eastern Time on **July 14, 2023**. 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, and Isabel Van Wyk – for their outstanding support in preparing this document for publication and 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] The security requirements for safeguarding CUI in nonfederal systems and organizations are derived from FIPS 199 [6], FIPS 200 [7], and NIST SP 800-53 [8] to maintain a consistent level of protection.

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 the CUI is resident in a nonfederal system and organization
- When the nonfederal organization is *not* 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 law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under E.O. 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] An *information system* is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems, such as industrial/process control systems, cyber-physical systems, embedded systems, and devices. 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 all types of computing platforms that can process, store, or transmit CUI.

[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 requirements* refers to the protection needs for a system or organization. Security requirements may be derived from many sources (e.g., laws, Executive Orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).

[7] In accordance with E.O. 13526 [2] and 32 CFR 2002 [5], the scope of CUI protection is limited to *confidentiality*. However, the security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms at the system level 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].

- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI registry

The security requirements in this publication are *only* applicable to components of nonfederal systems[9] that process, store, or transmit CUI *or* that provide protection for such components.[10] The requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations.

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] Nonfederal systems include information technology (IT) systems, operational technology (OT) systems, and Internet of Things (IoT) devices. NIST SP 800-82 [10] provides guidance for mitigating risks to OT systems.

[10] 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[11] criteria applied to the requirements and controls in FIPS 200 [7] and NIST SP 800-53 [8].

2.1. Basic Assumptions

The recommended 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*.[12]

2.2. Security Requirement Development Methodology

Starting with the NIST SP 800-53 security controls in the NIST SP 800-53B [13] moderate control baseline, which satisfy the minimum-security requirements in FIPS 200, 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
- Expected to be implemented by nonfederal organizations without specification by the Federal Government

The NIST SP 800-171 security requirements represent a subset of the controls that are necessary for a comprehensive information security program. The security requirements are organized into 17 families, as illustrated in Table 1. Each family contains the particular 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]

[11] The term *tailoring* is the process by which security and privacy control baselines are modified to achieve certain organizational goals and objectives [13].

[12] In accordance with 32 CFR 2002 [5], CUI is categorized at no less than the moderate confidentiality impact value as defined in FIPS 199 [6]. 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 these will be followed.

[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.

77 **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

78

79 For some requirements, *organization-defined parameters* (ODP) are included. These ODPs
80 provide additional flexibility by allowing federal organizations to specify values for the
81 designated parameters, as needed. Flexibility is achieved using *assignment* and *selection*
82 operations. The assignment and selection operations provide the capability to customize the
83 requirements based on organizational protection needs. Determination of organization-defined
84 parameter values can be guided and informed by laws, Executive Orders, directives, regulations,
85 policies, standards, guidance, or mission and business needs. Once specified, the values for the
86 organization-defined parameters become part of the requirement.

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

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

96 **3.1.8 Unsuccessful Logon Attempts**

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

99 **DISCUSSION**

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

105 **REFERENCES**

106 Source Controls: AC-7
107 Supporting Publications: SP 800-63-3 [28], SP 800-124 [29]

108 Appendix C provides a list of the controls from NIST SP 800-53 that support the security
109 requirements and those controls that have been eliminated from the moderate baseline based on
110 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* means a nonfederal system that processes, stores, or transmits CUI.

3.1. Access Control

3.1.1. Account Management

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

b. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined 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 accounts.

f. Disable accounts of individuals within [*Assignment: organization-defined time period*] when the accounts:

   1. Have expired;
   2. Are no longer associated with a user or individual;
   3. Are in violation of organizational policy; or
   4. Have been inactive for [*Assignment: organization-defined time period*].

g. Disable accounts of individuals within [*Assignment: organization-defined time period*] of discovery of [*Assignment: organization-defined significant risks*].

h. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*]:

   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When system usage or need-to-know changes for an individual.

DISCUSSION

This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations other than those determined by account type (e.g., privileged access, non-privileged access) are addressed in requirement 3.1.2. System account types include individual, shared, 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 shared, group, emergency, guest, anonymous, and temporary.

Organizations may choose to define access privileges or other attributes by account, by 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-related requirements (e.g., system upgrades, scheduled maintenance) and mission and business requirements (e.g., time zone differences, remote access to support 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, system administrators, legal staff, and human resource managers is essential when disabling system accounts for high-risk individuals. Time periods for notification of organizational personnel or roles may vary.

REFERENCES

Source Controls: AC-2, AC-2(3), AC-2(13)
Supporting Publications: SP 800-46 [15], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18], SP 800-77 [19], SP 800-113 [20], SP 800-114 [21], SP 800-121 [22], SP 800-162 [23], SP 800-178 [24], SP 800-192 [25], IR 7874 [26], IR 7966 [27]

3.1.2. Access Enforcement

Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

DISCUSSION

Access control policies control access between active entities or subjects (i.e., users or 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 level 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 Controls: AC-3, AC-17
Supporting Publications: SP 800-46 [15], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18], SP 800-77 [19], SP 800-113 [20], SP 800-114 [21], SP 800-121 [22], SP 800-162 [23], SP 800-178 [24], SP 800-192 [25], IR 7874 [26], IR 7966 [27]

3.1.3. Flow Enforcement

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

DISCUSSION

Information flow control regulates where information 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 the following: keeping export-controlled information from being transmitted in the clear to the internet, blocking outside traffic that claims to be from within the organization, restricting requests to the internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., encrypted tunnels, routers, gateways, and firewalls) that employ 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 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 Controls: AC-4
Supporting Publications: SP 800-160-1 [12], SP 800-162 [23], SP 800-178 [24]

3.1.4. Separation of Duties

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 helps reduce 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, testing, system management, programming, and network security), and ensuring that security 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.

REFERENCES

Source Controls: AC-5
Supporting Publications: SP 800-162 [23], SP 800-178 [24]

3.1.5. Least Privilege

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

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

c. Review [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] 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 processes. Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Least privilege is also applied to the development, implementation, and operation of the system.

REFERENCES

Source Controls: AC-6, AC-6(1), AC-6(7)
Supporting Publications: None

3.1.6. Least Privilege – Privileged Accounts

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

b. Require that users of system accounts (or roles) with access to [*Assignment: organization-defined security functions or security-relevant information*] use non-privileged accounts or roles when accessing nonsecurity functions.

DISCUSSION

Privileged accounts, including super user accounts, are typically described as system administrator accounts for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents nonprivileged users from accessing privileged information or privileged functions. In restricting privileged accounts, organizations may differentiate between allowed privileges for local accounts and domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of 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-6(2), AC-6(5)
Supporting Publications: None

3.1.7. Least Privilege – Privileged Functions

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 appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2.

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 risk from insider threats and advanced persistent threats.

REFERENCES

Source Controls: AC-6(9), AC-6(10)
Supporting Publications: None

3.1.8. Unsuccessful Logon Attempts

Limit the number of consecutive invalid logon attempts by a user 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 Controls: AC-7
Supporting Publications: SP 800-63-3 [28], SP 800-124 [29]

3.1.9. System Use Notification

Display system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable CUI rules.

DISCUSSION

System use notifications can be implemented using messages or warning banners that are displayed before individuals log in to the system. System use notifications are used only for access via logon interfaces with human users and are not required when human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network

logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for a legal review and approval of warning banner content.

REFERENCES

Source Controls: AC-8
Supporting Publications: None

3.1.10. Device Lock

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 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(1)
Supporting Publications: None

3.1.11. Session Termination

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

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 3.13.9. A logical session is initiated whenever a user (or process acting on behalf of a user) accesses a system. Such sessions can be terminated (and terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events 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 Controls: AC-12
Supporting Publications: None

3.1.12. Remote Access

a. Establish, authorize, and document usage restrictions, configurations, and connections allowed for each type of permitted remote access.

b. Monitor and control remote access methods.

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

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

e. Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

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 help ensure compliance with remote access policies. This occurs by auditing the connection activities of remote users on a variety of systems, including servers, notebook computers, workstations, smart phones, and tablets. Routing remote access through managed access control points enhances explicit control over such connections. It also reduces the 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 not able to execute such commands with the potential to do serious or catastrophic damage to the system.

REFERENCES

Source Controls: AC-17, AC-17(1), AC-17(3), AC-17(4)
Supporting Publications: SP 800-46 [15], SP 800-77 [19], SP 800-113 [20], SP 800-114 [21], SP 800-121 [22], IR 7966 [27]

3.1.13. Withdrawn: Incorporated into 3.1.12.

3.1.14. Withdrawn: Incorporated into 3.1.12.

3.1.15. Withdrawn: Incorporated into 3.1.12.

3.1.16. Wireless Access

a. Establish configuration requirements, connection requirements, and implementation guidance for wireless access to the system.

b. Authorize wireless access to the system prior to allowing such connections.

c. Protect wireless access to the system using authentication and encryption.

d. Disable, when not intended for use, wireless networking capabilities embedded within the system prior to issuance and deployment.

DISCUSSION

Establishing usage restrictions, configuration requirements, and connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. These restrictions and requirements help to reduce the 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 wide variety of devices that are part of the Internet of Things with potential wireless access to the system. 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 organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

REFERENCES

Source Controls: AC-18, AC-18(1), AC-18(3)
Supporting Publications: SP 800-94 [33], SP 800-97 [34], SP 800-124 [29]

3.1.17. Withdrawn: Incorporated into 3.1.16.

3.1.18. Access Control for Mobile Devices

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

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

c. Implement [*Selection: full-device encryption; 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 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/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 and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of 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 and computing platforms. Container-based encryption provides a fine-grained approach to the encryption of data and information, including encrypting selected data structures such as files, records, or fields.

REFERENCES

Source Controls: AC-19, AC-19(5)
Supporting Publications: SP 800-114 [35], SP 800-124 [29]

3.1.19. Withdrawn: Incorporated into 3.1.18.

3.1.20. Use of External Systems

a. [*Selection (one or more): Establish* [*Assignment: organization-defined terms and conditions*]*; Identify* [*Assignment: organization-defined controls asserted to be implemented on external systems*]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

   1. Access the system from external systems; and

   2. Process, store, or transmit CUI using external systems; or

b. Prohibit the use of [*Assignment: organizationally-defined types of external systems*].

DISCUSSION

External systems are systems that are used by but are not part of the organizational system and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. 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 any external system that is not organizationally owned or prohibit the use of personally owned systems).

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.

REFERENCES

Source Controls: AC-20
Supporting Publications: None

3.1.21. External Systems – Limits and Restrictions on Authorized Use

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

   1. Implemented controls on the external system as specified in the organization's security policies and security plans are verified; or

   2. Approved system connection or processing agreements with the organizational entity hosting the external system are retained.

b. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems as follows: [*Assignment: organization-defined usage restrictions*].

DISCUSSION

Limiting authorized use recognizes circumstances in which individuals who use external systems may need to access the organizational system. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm the system. Verification that the required controls have been implemented can be achieved through independent assessments, attestations, or other means, depending on the confidence level required by the organization. Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions.

REFERENCES

Source Controls: AC-20(1), AC-20(2)
Supporting Publications: None

3.1.22. Publicly Accessible Content

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

b. Review the content on publicly accessible systems for CUI [*Assignment: organization-defined frequency*] 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 Controls: AC-22
Supporting Publications: None

3.1.23. Account Management – Inactivity Logout

Require that users log out of the system [*Selection (one or more): after* [*Assignment: organization-defined time period*] *of expected inactivity*; *when* [*Assignment: organization-defined circumstances occur*]].

DISCUSSION

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by 3.1.10.

REFERENCES

Source Controls: AC-2(5)
Supporting Publications: SP 800-162 [23], SP 800-178 [24], SP 800-192 [25]

3.2. Awareness and Training

3.2.1. Literacy Training and Awareness

a. Provide security literacy training to system users:
   1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter; and
   2. When required by system changes or following [*Assignment: organization-defined events*].

b. Update training and awareness content [*Assignment: organization-defined fre*quency] and following [*Assignment: organization-defined events*].

DISCUSSION

Organizations provide basic and advanced levels of 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 and awareness 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 suspected incidents. The content also addresses the need for operations security and the handling of CUI.

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. Literacy training is conducted at a frequency consistent with applicable laws, directives, regulations, and policies. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

REFERENCES

Source Controls: AT-2
Supporting Publications: SP 800-50 [36]

3.2.2. Role-Based Training

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

   1. Before authorizing access to the system, CUI, or performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter; and

   2. When required by system changes.

b. Update role-based training content [*Assignment: organization-defined frequency*] 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 organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system 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 Controls: AT-3
Supporting Publications: SP 800-161 [37], SP 800-181 [38]

3.2.3. Advanced Literacy Training

Provide literacy training on recognizing and reporting potential and actual indicators of insider threat, social engineering, and social mining.

DISCUSSION

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

social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to effectively communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

REFERENCES

Source Controls: AT-2(2), AT-2(3)
Supporting Publications: SP 800-50 [36], SP 800-160-2 [11]

3.3. Audit and Accountability

3.3.1. Event Logging

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

b. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

DISCUSSION

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events that are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the system monitoring and auditing that are appropriate for each of the CUI 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 Controls: AU-2
Supporting Publications: SP 800-92 [39]

3.3.2. Audit Record Content

Include the following content in audit records: what type of event occurred; when and where the event occurred; source and outcome of the event; identity of individuals, subjects, objects, or entities associated with the event; and [*Assignment: organization-defined additional information*].

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, filenames, 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-3, AU-3(1)
Supporting Publications: None

3.3.3. Audit Record Generation

a. Provide an audit record generation capability for the event types defined in 3.3.1a.

b. Generate audit records for the event types defined in 3.3.1a. that include the audit record content defined in 3.3.2.

c. Retain audit records for [*Assignment: organization-defined time period consistent with records retention policy, applicable contract requirement, law, or regulation*].

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 access control or flow control rules invoked and 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 [39]

3.3.4. Response to Audit Logging Process Failures

a. Alert [*Assignment: organization-defined 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 Controls: AU-5
Supporting Publications: None

3.3.5. Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications and potential impact of inappropriate or unusual activity.

b. Report findings to [*Assignment: organization-defined 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 covers information security-related 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 non-local maintenance, system component inventory, mobile device connection, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and the use of mobile code. Findings can be reported to organizational entities that include 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 do not operate independently but rather collectively create a more complete view of events. Regarding the assessment of a given system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

REFERENCES

Source Controls: AU-6(3)
Supporting Publications: SP 800-86 [40], SP 800-101 [41]

3.3.6. Audit Record Reduction and Report Generation

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

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

DISCUSSION

Audit record reduction is a process that manipulates collected audit information and organizes it in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always come from the same system or organizational entities that

conduct auditing activities. An audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. The time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

REFERENCES

Source Controls: AU-7
Supporting Publications: None

3.3.7. Time Stamps

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

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

   1. Use Coordinated Universal Time (UTC);
   2. Have a fixed local time offset from UTC; or
   3. Include the local time offset as part of the time stamp.

DISCUSSION

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

REFERENCES

Source Controls: AU-8, SC-45, SC-45(1)
Supporting Publications: None

3.3.8. Protection of Audit Information

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

DISCUSSION

Audit information includes 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 system 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 controls.

REFERENCES

Source Controls: AU-9

Supporting Publications: None

3.3.9. Audit Information Access

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

DISCUSSION

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-9(4)
Supporting Publications: None

3.4. Configuration Management

3.4.1. Baseline Configuration

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

b. Review and update the baseline configuration of the system [*Assignment: organization-defined frequency*] and when system components are installed or upgraded.

DISCUSSION

Baseline configurations for systems and system components include aspects of connectivity, operation, and communications. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security control implementations, information about system components, operational procedures, network topology, and the logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

REFERENCES

Source Controls: CM-2
Supporting Publications: SP 800-124 [29], SP 800-128 [45], IR 8011-2 [46], IR 8011-3 [47]

3.4.2. Configuration Settings

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

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

c. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

DISCUSSION

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. 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 systems, including the parameters required to satisfy other security requirements. Security parameters include registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, 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 Controls: CM-6
Supporting Publications: SP 800-70 [48], SP 800-126 [49], SP 800-128 [45]

3.4.3. Configuration Change Control

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

REFERENCES

Source Controls: CM-3
Supporting Publications: SP 800-124 [29], SP 800-128 [45]

3.4.4. Impact Analyses

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

b. After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting specified security requirements.

DISCUSSION

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

REFERENCES

Source Controls: CM-4, CM-4(2)
Supporting Publications: SP 800-128 [45]

3.4.5. Access Restrictions for Change

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 systems or the operational procedures related to the systems can have potentially significant effects on the security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems 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 systems), and change windows (i.e., changes occur only during specified times).

REFERENCES

Source Controls: CM-5
Supporting Publications: FIPS 140-3 [42], FIPS 180-4 [43], SP 800-128 [45]

3.4.6. Least Functionality

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

b. Prohibit or restrict use of the following functions, ports, protocols, software, and/or services: [*Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services*].

c. Prevent program execution in accordance with [*Selection (one or more):* [*Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions*]*; rules authorizing the terms and conditions of software program usage*].

d. Review the system [*Assignment: organization-defined frequency*] to identify and disable/remove functions, ports, protocols, software, and/or services identified in 3.4.6b.

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 systems 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, the transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections (e.g., firewalls and host-based intrusion detection systems) to identify and prevent the use of prohibited functions, ports, protocols, and services.

Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution, prohibiting auto-execute, and restricting the number of program instances executed at the same time. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols that organizations consider eliminating, restricting, or disabling.

REFERENCES

Source Controls: CM-7, CM-7(1), CM-7(2)
Supporting Publications: SP 800-160-1 [12], SP 800-167 [50]

3.4.7. Withdrawn: Incorporated into 3.4.6.

3.4.8. Authorized Software – Allow by Exception

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

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

c. Review and update the list of authorized software programs [*Assignment: organization-defined frequency*].

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 Controls: CM-7(5)
Supporting Publications: SP 800-160-1 [12], SP 800-167 [50]

3.4.9. User-Installed Software

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through the following methods: [*Assignment: organization-defined methods*].

c. Monitor policy compliance [*Assignment: organization-defined frequency*].

DISCUSSION

Users can install software if provided the necessary privileges. 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 sources. Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. 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.

REFERENCES

Source Controls: CM-11
Supporting Publications: None

3.4.10. System Component Inventory

a. Develop and document an inventory of system components.

b. Review and update the system component inventory [*Assignment: organization-defined frequency*] and as part of component installations, removals, and system updates.

DISCUSSION

System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational 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 across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include the date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

REFERENCES

Source Controls: CM-8, CM-8(1)
Supporting Publications: SP 800-124 [29], SP 800-128 [45], IR 8011-2 [46], IR 8011-3 [47]

3.4.11. Information Location

a. Identify and document the location within the system where CUI is processed and stored.

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

c. Document changes to the location 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 Controls: CM-12
Supporting Publications: None

3.4.12. System and Component Configuration for High-Risk Areas

a. Issue [*Assignment: organization-defined system*] with [*Assignment: organization-defined system configurations*] to individuals traveling to locations that the organization deems to be of significant risk.

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

DISCUSSION

When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat. For example, organizations can take actions for notebook computers 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 components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives.

REFERENCES

Source Controls: CM-2(7)
Supporting Publications: SP 800-124 [29], SP 800-128 [45]

3.5. Identification and Authentication

3.5.1. User Identification, Authentication, and Re-Authentication

a. Uniquely identify and authenticate system user, 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 employees or individuals who have equivalent status to employees. Typically, individual identifiers are the usernames associated with the system accounts assigned to those individuals. Since 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 require the re-authentication of 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-2, IA-11
Supporting Publications: SP 800-63-3 [28]

3.5.2. Device Identification and Authentication

Uniquely identify and authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing a system or network 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.

REFERENCES

Source Controls: IA-3
Supporting Publications: SP 800-63-3 [28]

3.5.3. Multi-Factor Authentication

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-2(1), IA-2(2)
Supporting Publications: SP 800-63-3 [28]

3.5.4. Replay-Resistant Authentication

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 Controls: IA-2(8)
Supporting Publications: SP 800-63-3 [28]

3.5.5. Identifier Management

a. Receive authorization from [*Assignment: organization-defined 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. Identify the status of each individual with the following characteristic: [*Assignment: organization-defined characteristic*].

DISCUSSION

Identifiers are provided for users, processes acting on behalf of users, and devices. Preventing the reuse of identifiers implies preventing 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, it might be useful for an employee to know that one of the individuals on an email message is a contractor.

REFERENCES

Source Controls: IA-4, IA-4(4)
Supporting Publications: SP 800-63-3 [28]

3.5.6. Withdrawn.

3.5.7. Password Management

a. Enforce the following password composition and complexity rules: [*Assignment: organization-defined composition and complexity rules*].

b. Allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

d. Transmit passwords only over cryptographically-protected channels.

e. Store passwords using an approved salted key derivation function, preferably using a keyed hash.

f. Select a new password immediately upon account recovery.

g. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

DISCUSSION

Password-based authentication applies to passwords used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over 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.

REFERENCES

Source Controls: IA-5(1)
Supporting Publications: SP 800-63-3 [28]

3.5.8. Withdrawn.

3.5.9. Withdrawn: Incorporated into 3.5.7.

3.5.10. Withdrawn: Incorporated into 3.5.7.

3.5.11. Authentication Feedback

Obscure feedback of authentication information.

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 authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a limited time before fully obscuring it.

REFERENCES

Source Controls: IA-6
Supporting Publications: None

3.5.12. Authenticator Management

a. Establish initial authenticator content for any authenticators issued by the organization.

b. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.

c. Establish and implement administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators.

d. Protect authenticator content from unauthorized disclosure and modification.

e. Change default authenticators prior to first use.

f. Change or refresh authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*].

g. Change authenticators for group or role accounts when membership to those accounts change.

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 3.15.3 for authenticators in the possession of individuals and by 3.1.1, 3.1.2, 3.1.5, and 3.13.8 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 safeguard 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.

REFERENCES

Source Controls: IA-5, IA-5(6)
Supporting Publications: None

3.6. Incident Response

3.6.1. Incident Response Plan and Handling

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-4, IR-8
Supporting Publications: SP 800-50 [36], SP 800-61 [51], SP 800-161 [37]

3.6.2. Incident Monitoring, Reporting, and Response Assistance

a. Track and document system security incidents.

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

c. 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 a variety of 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 designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and 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 forensics services or consumer redress services, when required.

REFERENCES

Source Controls: IR-5, IR-6, IR-7
Supporting Publications: SP 800-61 [51], SP 800-86 [40]

3.6.3. Incident Response Testing

Test the effectiveness of the incident response capability [*Assignment: organization-defined frequency*].

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. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

REFERENCES

Source Controls: IR-3
Supporting Publications: SP 800-84 [52]

3.6.4. Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities.

b. Review and update incident response training content [*Assignment: organization-defined frequency*] 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 who 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 3.2.2. 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 Controls: IR-2
Supporting Publications: SP 800-86 [40], SP 800-137 [53]

3.7. Maintenance

3.7.1. Withdrawn: Recategorized as NCO.

3.7.2. Withdrawn: Incorporated into 3.7.4 and 3.7.6.

3.7.3. Withdrawn: Incorporated into 3.8.3.

3.7.4. Maintenance Tools

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

b. Inspect maintenance tools and media containing diagnostic and test programs for malicious code before the media and tools are used in the system.

c. Prevent the removal of maintenance equipment containing CUI by:

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

   2. Sanitizing or destroying the equipment; or

   3. Obtaining an exemption from [*Assignment: organization-defined officials*] explicitly authorizing removal of the equipment from 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, upon inspection of media that contain maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures. A periodic review of system maintenance tools can result in the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. 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) are not addressed by maintenance tools.

REFERENCES

Source Controls: MA-3, MA-3(1), MA-3(2), MA-3(3)
Supporting Publications: SP 800-88 [54]

3.7.5. Nonlocal Maintenance

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 either 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 3.5.1.

REFERENCES

Source Controls: MA-4
Supporting Publications: SP 800-63-3 [28], SP 800-88 [54]

3.7.6. Maintenance Personnel

a. Establish a process for maintenance personnel authorization, and maintain a list of authorized maintenance organizations or personnel.

b. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.

c. 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 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the system. 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 not 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 Controls: MA-5
Supporting Publications: None

3.8. Media Protection

3.8.1. Media Storage

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

DISCUSSION

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.

REFERENCES

Source Controls: MP-4
Supporting Publications: SP 800-111 [55]

3.8.2. Media Access

Restrict access to CUI on digital and non-digital media to [*Assignment: organization-defined personnel or roles*].

DISCUSSION

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 Controls: MP-2
Supporting Publications: SP 800-111 [55]

3.8.3. Media Sanitization

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

DISCUSSION

Media sanitization applies to all digital and non-digital system 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 system media such that the information cannot be retrieved or reconstructed. Sanitization techniques (e.g., clearing, purging, cryptographically erasing, and destroying) prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods with the recognition that destruction is sometimes necessary

when other methods cannot be applied to media that require sanitization. NARA policies control the sanitization process for CUI.

REFERENCES

Source Controls: MP-6
Supporting Publications: SP 800-88 [54]

3.8.4. Media Marking

a. Mark system media containing CUI indicating distribution limitations, handling caveats, and security markings.

b. Exempt [*Assignment: organization-defined types of system media containing CUI*] from marking if the media remain within [*Assignment: organization-defined controlled areas*].

DISCUSSION

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 appropriate safeguarding and dissemination requirements for such information.

REFERENCES

Source Controls: MP-3
Supporting Publications: None

3.8.5. Media Transport

a. Protect, control, and maintain accountability for system media containing CUI and during transport outside of controlled areas.

b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI stored on digital media during transport.

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 controls to meet the requirements established for protecting information and systems. Controls to protect media during transport include cryptography and 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 system 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.

REFERENCES

Source Controls: MP-5, SC-28, SC-28(1)
Supporting Publications: SP 800-111 [55]

3.8.6. Withdrawn: Incorporated into 3.8.5.

3.8.7. Media Use

a. [*Selection: Restrict; Prohibit*] the use of [*Assignment: organization-defined removable system media*].

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

DISCUSSION

In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, such as restricting or prohibiting the use of flash drives or external hard drives. Organizations can employ technical and nontechnical controls (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. Finally, organizations may 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. Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

REFERENCES

Source Controls: MP-7
Supporting Publications: SP 800-111 [55]

3.8.8. Withdrawn: Incorporated into 3.8.7.

3.8.9. System Backup – Cryptographic Protection

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

DISCUSSION

Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backed-up information that contains CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

REFERENCES

Source Controls: CP-9(8)
Supporting Publications: SP 800-34 [56], SP 800-130 [57], SP 800-152 [58]

3.9. Personnel Security

3.9.1. Personnel Screening

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. The screening 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 Controls: PS-3
Supporting Publications: SP 800-181 [38]

3.9.2. Personnel Termination and Transfer

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 all security-related system property.

b. When individuals are reassigned or transferred to other positions within 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 formal transfer action*]; and
3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

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-4, PS-5
Supporting Publications: None

3.9.3. External Personnel Security

a. Establish and document personnel security requirements, including security roles and responsibilities for external providers.

b. Require external providers to comply with the personnel security policies and procedures established by the organization.

c. Monitor provider compliance with personnel security requirements.

DISCUSSION

External providers include contractors and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, cloud services, and network or security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel who work at organizational facilities with credentials, badges, or system privileges issued by organizations.

REFERENCES

Source Controls: PS-7
Supporting Publications: None

3.10. Physical Protection

3.10.1. Physical Access Authorizations

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

b. Issue authorization credentials for facility access.

c. Review the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*].

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

DISCUSSION

Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed 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 Controls: PE-2
Supporting Publications: None

3.10.2. Monitoring Physical Access

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

b. Review physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*].

c. Coordinate the results of reviews and investigations with the organizational incident response capability.

DISCUSSION

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. Organizational incident response capabilities include investigations of physical security incidents and responses to the 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 Controls: PE-6
Supporting Publications: None

3.10.3. Withdrawn: Incorporated into 3.10.7.

3.10.4. Withdrawn: Incorporated into 3.10.7.

3.10.5. Withdrawn: Incorporated into 3.10.7.

3.10.6. Alternate Work Site

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

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

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 sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

REFERENCES

Source Controls: PE-17
Supporting Publications: SP 800-46 [15], SP 800-114 [21]

3.10.7. Physical Access Control

a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] by:

   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress and egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards*].

b. Maintain physical access audit logs for [*Assignment: organization-defined 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

Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. 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 facility access points, interior access points to systems that require supplemental access controls, or both.

REFERENCES

Source Controls: PE-3
Supporting Publications: None

3.10.8. Access Control for Transmission and Output Devices

a. Control physical access to system distribution and transmission lines within organizational facilities.

b. Control physical access to output from [*Assignment: organization-defined output devices*] to prevent unauthorized individuals from obtaining the output.

DISCUSSION

Safeguarding measures applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or the modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by 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-4, PE-5
Supporting Publications: None

3.11. Risk Assessment

3.11.1. Risk Assessment

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

b. Update risk assessments (including supply chain risk) [*Assignment: organization-defined frequency*].

DISCUSSION

Clearly defined system boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets based on the operation and use of the system. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level and at any phase in the system development life cycle.

Risk assessments include supply chain-related risks associated with suppliers or contractors and the system, system component, or system service that they provide. Supply chain events that affect risk include disruption, the use of defective components, the insertion of counterfeits, theft, malicious development practices, improper delivery practices, and the insertion of malicious code. These events can have a significant impact on the system and its information and, therefore, can also adversely impact organizations. The supply chain events may be unintentional or malicious and can occur at any point in the system life cycle.

REFERENCES

Source Controls: RA-3, RA-3(1), SR-6
Supporting Publications: SP 800-30 [59], SP 800-161 [37]

3.11.2. Vulnerability Monitoring and Scanning

a. Monitor and scan for vulnerabilities in the system [*Assignment: organization-defined frequency*] and when new vulnerabilities affecting the system are identified.

b. Remediate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.

c. Update vulnerabilities to be scanned [*Assignment: organization-defined frequency*].

d. Implement privileged access authorization to the system for vulnerability scanning activities.

DISCUSSION

Organizations determine the required vulnerability scanning for system components (including hardware, software, firmware, and applications) and ensure that potential sources of vulnerabilities (e.g., networked printers, scanners, and copiers) are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered and announced and new scanning methods are developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible.

Vulnerability analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers). Vulnerability scanning includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, as well as scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

REFERENCES

Source Controls: RA-5, RA-5(2), RA-5(5)
Supporting Publications: SP 800-40 [60], SP 800-53A [61], SP 800-70 [48], SP 800-115 [62], SP 800-126 [49]

3.11.3. Withdrawn: Incorporated into 3.11.2.

3.11.4. Risk Response

Respond to findings from security assessments, monitoring, and audits.

DISCUSSION

Organizations have many options for responding to risk, including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The organizational risk management strategy and risk tolerance influence risk response decisions and actions. This requirement addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

REFERENCES

Source Controls: RA-7
Supporting Publications: SP 800-30 [59], SP 800-37 [63], SP 800-39 [64], SP 800-160-1 [12]

3.12. Security Assessment and Monitoring

3.12.1. Control Assessments

Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting specified security requirements.

DISCUSSION

Organizations assess security controls in the system and the environment in which that system operates as part of the system development life cycle. Security controls are the safeguards that organizations implement to satisfy security requirements. By assessing implemented security controls, organizations determine whether the necessary safeguards are in place and operating as intended. Security control assessments identify weaknesses and deficiencies early in the system life cycle, provide essential information needed to make risk-based decisions, and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security posture of the system during the system life cycle.

REFERENCES

Source Controls: CA-2
Supporting Publications: SP 800-53 [8], SP 800-53A [61], SP 800-37 [63], SP 800-115 [62]

3.12.2. Plan of Action and Milestones

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 control assessments; and
   2. To reduce or eliminate known vulnerabilities in the system.

b. Update the existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control 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 unimplemented security requirements and security controls 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 chosen 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 Controls: CA-5
Supporting Publications: SP 800-37 [63]

3.12.3. Continuous Monitoring

Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and assessment of control effectiveness.

DISCUSSION

Continuous monitoring at the system level facilitates ongoing awareness of the system security posture to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root cause analysis may be needed to determine the specific control that has failed.

REFERENCES

Source Controls: CA-7
Supporting Publications: SP 800-37 [63], SP 800-39 [64], SP 800-53A [61], SP 800-115 [62], SP 800-137 [53]

3.12.4. Withdrawn: Incorporated into 3.15.2.

3.12.5. Independent Assessment

Use independent assessors or assessment teams to assess controls.

DISCUSSION

Independent assessors or assessment teams are individuals or groups who conduct impartial security assessments of the system. Impartiality means that assessors are free from perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the system under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations that acquire their services.

REFERENCES

Source Controls: CA-2(1)
Supporting Publications: SP 800-37 [63], SP 800-53A [61], SP 800-115 [62], SP 800-137 [53]

3.12.6. Information Exchange

a. Approve, document, and manage the exchange of CUI between the system and other systems using [*Assignment: organization-defined agreements*].

b. Review and update the agreements [*Assignment: organization-defined frequency*].

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) or 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 Controls: CA-3
Supporting Publications: SP 800-47 [87]

3.12.7. Internal System Connections

a. Authorize internal system connections of [*Assignment: organization-defined system components or classes of components*].

b. Review the continued need for each internal system connection [*Assignment: organization-defined frequency*].

DISCUSSION

Internal system connections are connections between the organizational system and separate constituent system components (i.e., connections between components that are part of the same system), including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration.

REFERENCES

Source Controls: CA-9
Supporting Publications: SP 800-124 [29]

3.13. System and Communications Protection

3.13.1. Boundary Protection

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 networks or 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, guards, network-based malicious code analysis, virtualization systems, or 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. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

REFERENCES

Source Controls: SC-7

Supporting Publications: SP 800-41 [68], SP 800-125B [69], SP 800-160-1 [12], SP 800-189 [71], SP 800-207 [70]

3.13.2. Withdrawn: Incorporated into 3.16.1.

3.13.3. Separation of System and User Functionality

Separate user functionality from system management functionality.

DISCUSSION

System management functionality includes the functions necessary to administer databases, network components, workstations, or servers and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement the separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. The separation of functionality may include isolating administrative interfaces on different domains and with additional access controls.

REFERENCES

Source Controls: SC-2
Supporting Publications: SP 800-160-1 [12]

3.13.4. Information in Shared System Resources

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 Controls: SC-4
Supporting Publications: None

3.13.5. Withdrawn: Incorporated into 3.13.1.

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

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 Controls: SC-7(5)
Supporting Publications: SP 800-41 [68], SP 800-77 [19], SP 800-189 [71]

3.13.7. Split Tunneling

Prevent split tunneling for remote devices unless the split tunnel is securely provisioned using [*Assignment: organization-defined safeguards*].

DISCUSSION

Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate with a resource in an external network via some other connection. This method of network access enables a user to access remote devices and simultaneously access uncontrolled networks. Split tunneling may be desirable by remote users to communicate with system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections and make the system vulnerable to attack and the exfiltration of CUI.

Split tunneling can be prevented by disabling configuration settings that allow such capabilities in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved through the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments or to a specific set of pre-approved addresses without user control.

REFERENCES

Source Controls: SC-7(7)
Supporting Publications: SP 800-41 [68], SP 800-77 [19], SP 800-189 [71]

3.13.8. Transmission and Storage Confidentiality

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. Communication paths outside of the physical protection of controlled boundaries are susceptible to both interception and modification. Encryption protects CUI from unauthorized disclosure during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPsec. Cryptographic standards include FIPS-validated cryptography [30] [31] [32] and NSA-approved cryptography. Information at rest refers to the state of CUI when it resides on the system and is not in process or in transit, including internal or external storage devices, storage area network devices, and databases. The focus of protecting CUI at rest is not on the type of storage device or the frequency of access to that device but rather on the state of the information.

REFERENCES

Source Controls: SC-8(1), SC-28(1)
Supporting Publications: FIPS 140-3 [42], FIPS 197 [72], SP 800-46 [15], SP 800-52 [73], SP 800-56A [77], SP 800-56B [78], SP 800-56C [79], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18], SP 800-77 [19], SP 800-111 [55], SP 800-113 [20], SP 800-114 [21], SP 800-121 [22], SP 800-124 [29], SP 800-177 [74]

3.13.9. Network Disconnect

Terminate network connections associated with communications sessions at the end of the sessions or after [*Assignment: organization-defined time period*] of inactivity.

DISCUSSION

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

REFERENCES

Source Controls: SC-10
Supporting Publications: None

3.13.10. Cryptographic Key Establishment and Management

Establish and manage cryptographic keys when cryptography is implemented in the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

DISCUSSION

Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters.

REFERENCES

Source Controls: SC-12

Supporting Publications: FIPS 140-3 [42], SP 800-56A [77], SP 800-56B [78], SP 800-56C [79], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18], SP 800-63-3 [28]

3.13.11. Cryptographic Protection

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

DISCUSSION

Cryptography can be employed to support a variety of security solutions, including the protection of CUI. Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. FIPS-validated cryptography is described in [30] [31] [32].

REFERENCES

Source Controls: SC-13
Supporting Publications: FIPS 140-3 [42]

3.13.12. Collaborative Computing Devices and Applications

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*].

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

DISCUSSION

Collaborative computing devices include networked white boards, microphones, and cameras. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded. Solutions to prevent device usage include webcam covers and buttons to disable microphones.

REFERENCES

Source Controls: SC-15
Supporting Publications: None

3.13.13. Mobile Code

a. Define acceptable and unacceptable mobile code and mobile code technologies.

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

DISCUSSION

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. 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

as well as mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address the specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within the system, including requiring mobile code to be digitally signed by a trusted source.

REFERENCES

Source Controls: SC-18
Supporting Publications: SP 800-28 [75]

3.13.14. Withdrawn: Technology-specific.

3.13.15. Session Authenticity

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 validity of transmitted information. Authenticity protection includes protecting against "adversary-in-the-middle" attacks (also known as "man-in-the middle" attacks), session hijacking, and the insertion of false information into sessions.

REFERENCES

Source Controls: SC-23
Supporting Publications: SP 800-52 [73], SP 800-77 [19], SP 800-95 [76], SP 800-113 [20]

3.13.16. Withdrawn: Incorporated into 3.13.8.

3.13.17. Internal Network Communications Traffic

Route internal network communications traffic to external networks through an authenticated proxy server.

DISCUSSION

External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients who request system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential

for "adversary-in-the-middle" attacks (also known as "man-in-the middle attacks") depending on the implementation.

REFERENCES

Source Controls: SC-7(8)
Supporting Publications: SP 800-41 [68], SP 800-125B [69], SP 800-207 [70], SP 800-160-1 [12]

3.13.18. System Access Points

Limit the number of external network connections to the system.

DISCUSSION

Limiting the number of external network connections facilitates the monitoring of inbound and outbound communications traffic and is important during transition periods from older to newer technologies. Such transitions may require implementing older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

REFERENCES

Source Controls: SC-7(3)
Supporting Publications: SP 800-41 [68], SP 800-125B [69], SP 800-207 [70], SP 800-160-1 [12]

3.14. System and Information Integrity

3.14.1. Flaw Remediation

a. Identify, report, and correct system flaws.

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

c. 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 Controls: SI-2
Supporting Publications: SP 800-39 [64], SP 800-40 [60], SP 800-128 [45]

3.14.2. Malicious Code Protection

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 organizational configuration management policy and procedures.

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 a variety of ways, including by electronic mail, the world wide web, 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 as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls – including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices – to ensure that software does not perform functions other than the functions intended. Organizations may determine that different actions are warranted in response to the detection of malicious code. For example, organizations can define actions 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 Controls: SI-3
Supporting Publications: SP 800-83 [80], SP 800-125B [69], SP 800-177 [74]

3.14.3. Security Alerts, Advisories, and Directives

a. Receive security alerts, advisories, and directives from external organizations.

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

DISCUSSION

There are many publicly available sources of system security alerts and advisories. For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness across the Federal Government and in nonfederal organizations. Software vendors, subscription services, and industry Information Sharing and Analysis Centers (ISACs) may also provide

security alerts and advisories. 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. Examples of response actions include notifying relevant external organizations, such as external mission and business partners, supply chain partners, service providers, and peer or supporting organizations.

REFERENCES

Source Controls: SI-5
Supporting Publications: SP 800-161 [37]

3.14.4. Withdrawn: Incorporated into 3.14.2.

3.14.5. Withdrawn: Addressed by 3.14.2.

3.14.6. System Monitoring

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

DISCUSSION

System monitoring involves external and internal monitoring. External monitoring includes the observation of events that occur at the system boundary, while 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.

System monitoring is an integral part of continuous monitoring and incident response programs. The output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, internet). A remote connection is any connection with a device that communicates through an external network (e.g., the internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include 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-4, SI-4(4)
Supporting Publications: SP 800-61 [51], SP 800-83 [80], SP 800-92 [39], SP 800-94 [33], SP 800-137 [53], SP 800-177 [74]

3.14.7. Withdrawn: Incorporated into 3.14.6.

3.14.8. Spam Protection

a. Implement spam protection mechanisms at designated locations within the system to detect and act on unsolicited messages.

b. Update spam protection mechanisms [*Assignment: organization-defined frequency*].

DISCUSSION

System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

REFERENCES

Source Controls: SI-8
Supporting Publications: SP 800-45 [81], SP 800-177 [74]

3.15. Planning

3.15.1. Policy and Procedures

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 [*Assignment: organization-defined frequency*].

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 CUI security requirements. Policies can be included as part of the generalized security policy or be represented by separate policies that address each family of security requirements. Procedures describe how policies, requirements, and controls 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-1, AT-1, AU-1, CA-1, CM-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1, SR-1
Supporting Publications: SP 800-12 [65], SP 800-100 [66]

3.15.2. System Security Plan

a. Develop and document a system security plan that describes:
   1. System boundary and operating environment;
   2. Security requirements, tailoring actions, and implementation; and
   3. Connections to other systems.

b. Review and update the plan at [*Assignment: organization-defined frequency*].

DISCUSSION

System security plans relate security requirements to a set of security controls. System security plans also provide a high-level description of how the controls meet those requirements but do not provide detailed descriptions of the design or implementation of the controls. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and 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 Controls: PL-2
Supporting Publications: SP 800-18 [67]

3.15.3. Rules of Behavior

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

b. Review and update the rules of behavior [*Assignment: organization-defined frequency*].

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 Controls: PL-4
Supporting Publications: SP 800-18 [67]

3.16. System and Services Acquisition

3.16.1. Security Engineering Principles

Apply systems security engineering principles in the specification, design, development, implementation, and modification of the system and system components.

DISCUSSION

Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build trustworthy secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

REFERENCES

Source Controls: SA-8
Supporting Publications: SP 800-160-1 [12], SP 800-160-2 [11], SP 800-207 [70]

3.16.2. Unsupported System Components

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

b. Provide options for alternative sources for continued support for unsupported components.

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 an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where 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, alternatively, 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 Controls: SA-22
Supporting Publications: None

3.16.3. External System Services

a. Require the providers of external system services to comply with organizational security requirements, and implement the following controls: [*Assignment: organization-defined controls*].

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services.

c. Implement the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [*Assignment: organization-defined processes, methods, and techniques*].

DISCUSSION

External system services are provided by an external provider, and in most cases, the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. 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 for the implemented controls, describe measurable outcomes, and identify remedies, mitigations, and response requirements for identified 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 the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

REFERENCES

Source Controls: SA-9
Supporting Publications: SP 800-160-1 [12], SP 800-161 [37]

3.17. Supply Chain Risk Management

3.17.1. Supply Chain Risk Management Plan

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

b. Review and update the plan [*Assignment: organization-defined frequency*].

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, insertion of malicious software 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 risk 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 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 SDLC 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 Controls: SR-2
Supporting Publications: SP 800-30 [59], SP 800-39 [64], SP 800-160-1 [12], SP 800-181 [38]

3.17.2. Acquisition Strategies, Tools, and Methods

Develop and implement acquisition strategies, contract tools, and procurement methods to protect against, identify, 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 Controls: SR-5
Supporting Publications: SP 800-30 [59], SP 800-161 [37]

3.17.3. Supply Chain Controls and Processes

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

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [*Assignment: organization-defined supply chain controls*].

DISCUSSION

Supply chain elements include organizations, entities, or tools that are employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security 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 Controls: SR-3
Supporting Publications: SP 800-30 [59], SP 800-161 [37]

3.17.4. Component Disposal

Dispose of system components, documentation, or tools containing CUI using the following techniques and methods: [*Assignment: organization-defined techniques and methods*].

DISCUSSION

Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, operations, or maintenance and include methods such as disk cleaning, the removal of cryptographic keys, the partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files, shipping and delivery documentation, memory sticks with software code, or complete routers or servers that include permanent media that contain sensitive or proprietary information. Additionally, the proper disposal of system components helps to prevent such components from entering the gray market.

REFERENCES

Source Controls: SR-12
Supporting Publications: SP 800-30 [59], SP 800-161 [37]

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 Transformation Initiative (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] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

[11] 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

[12] 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

[13] Joint Task Force Transformation Initiative (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

[14] Office of Management and Budget Memorandum 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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

[25] 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

[26] 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

[27] 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

[28] 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

[29] Souppaya MP, Scarfone KA (2013) 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. 1. https://doi.org/10.6028/NIST.SP.800-124r1

[30] National Institute of Standards and Technology (2019) Cryptographic Standards and Guidelines. Available at https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

[31] National Institute of Standards and Technology (2019) Cryptographic Algorithm Validation Program. Available at https://csrc.nist.gov/projects/cavp

[32] National Institute of Standards and Technology (2019) Cryptographic Module Validation Program. Available at https://csrc.nist.gov/projects/cmvp

[33] 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

[34] 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

[35] 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

[36] 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

[37] 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

[38] 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

[39] 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

[40] 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

[41] 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

[42] 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

[43] 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

[44] 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

[45] 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

[46] 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

[47] 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

[48] 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

[49] 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

[50] 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

[51] 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

[52] 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

[53] 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

[54] 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

[55] 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

[56] 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

[57] 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

[58] 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

[59] 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

[60] 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

[61] 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

[62] 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

[63] 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

[64] 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

[65] 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

[66] 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

[67] 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

[68] 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

[69] 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

[70] 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

[71] 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

[72] 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. https://doi.org/10.6028/NIST.FIPS.197

[73] 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

[74] 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

[75] 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

[76] 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

[77] 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

[78] 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

[79] 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

[80] 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

[81] 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

[82] Committee on National Security Systems (2015) 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

[83] 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

[84] 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

[85] 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

[86] 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

[87] 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

BYOD
Bring Your Own Device

CFR
Code of Federal Regulations

CISA
Cybersecurity and Infrastructure Security Agency

CNSS
Committee on National Security Systems

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

FOIA
Freedom of Information Act

FTP
File Transfer Protocol

GMT
Greenwich Mean Time

IEEE
Institute of Electrical and Electronics Engineers

IoT
Internet of Things

ISOO
Information Security Oversight Office

IT
Information Technology

ITL
Information Technology Laboratory

LSI
Large-Scale Integration

MAC
Media Access Control

NARA
National Archives and Records Administration

NFO
Nonfederal Organization

NIST
National Institute of Standards and Technology

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

SDLC
System Development Life Cycle

SP
Special Publication

TCP/IP
Transmission Control Protocol/Internet Protocol

TLS
Transport Layer Security

UTC
Coordinated Universal Time

VPN
Virtual Private Network

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 [82] 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. [14]

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. [83]

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. [64]

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

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [83]

configuration management
A collection of activities focused on establishing and maintaining the integrity of information technology products and systems through 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.

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. [84]

FIPS-validated cryptography
A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet 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*. [82]

hardware
The material physical components of a system. See *software* and *firmware*. [82]

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. [83]

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. [14]

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. [85]

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. [83]

information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [85]

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. [14]

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. [83]

internal network
A network where the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or 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 a network, either an external network (e.g., the internet) or an internal network.

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]

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. [14]

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 data or information (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 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 the 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. [14]

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. [59]

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

Process to remove information from media such that data recovery is not possible. It includes removing 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. [82]

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. [14]

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. [14]

security domain
A domain that implements a security policy and is administered by a single authority. Adapted from [82]

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.

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. [45]

system security plan
A document that describes how an organization meets the security requirements for a system or plans to meet the requirements. 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. [59]

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 lists the security controls in the NIST SP 800-53 moderate baseline [13]. The symbols in Table 2 are used in Table 3 through Table 22 to specify the tailoring actions taken to obtain the security requirements in Section 3. The security controls and control enhancements in the tables below 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. Tailoring criteria and associated symbols

TAILORING SYMBOL	TAILORING CRITERIA
NCO	Not directly related to protecting the confidentiality of CUI
NFO	Expected to be implemented by nonfederal organizations without specification
FED	Primarily the responsibility of the Federal Government
CUI	Directly related to protecting the confidentiality of CUI
NA	Not Applicable

Table 3. Access Control

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AC-1	Policy and Procedures	CUI	3.15.1
AC-2	Account Management	CUI	3.1.1
AC-2(1)	Account Management – Automated System Account Management	NCO	—
AC-2(2)	Account Management – Automated Temporary and Emergency Account Management	NCO	—
AC-2(3)	Account Management – Disable Accounts	CUI	3.1.1
AC-2(4)	Account Management – Automated Audit Actions	NCO	—
AC-2(5)	Account Management – Inactivity Logout	CUI	3.1.23
AC-2(13)	Account Management – Disable Accounts for High-Risk Individuals	CUI	3.1.1
AC-3	Access Enforcement	CUI	3.1.2
AC-4	Information Flow Enforcement	CUI	3.1.3
AC-5	Separation of Duties	CUI	3.1.4
AC-6	Least Privilege	CUI	3.1.5
AC-6(1)	Least Privilege – Authorize Access to Security Functions	CUI	3.1.5
AC-6(2)	Least Privilege – Non-Privileged Access for Nonsecurity Functions	CUI	3.1.6
AC-6(5)	Least Privilege – Privileged Accounts	CUI	3.1.6
AC-6(7)	Least Privilege – Review of User Privileges	CUI	3.1.5
AC-6(9)	Least Privilege – Log Use of Privileged Functions	CUI	3.1.7
AC-6(10)	Least Privilege – Prohibit Non-Privileged Users from Executing Privileged Functions	CUI	3.1.7
AC-7	Unsuccessful Logon Attempts	CUI	3.1.8
AC-8	System Use Notification	CUI	3.1.9

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AC-11	Device Lock	CUI	3.1.10
AC-11(1)	Device Lock – Pattern-Hiding Displays	CUI	3.1.10
AC-12	Session Termination	CUI	3.1.11
AC-14	Permitted Actions Without Identification or Authentication	FED	—
AC-17	Remote Access	CUI	3.1.2
AC-17(1)	Remote Access – Monitoring and Control	CUI	3.1.12
AC-17(2)	Remote Access – Protection of Confidentiality and Integrity Using Encryption	CUI	3.13.8
AC-17(3)	Remote Access – Managed Access Control Points	CUI	3.1.12
AC-17(4)	Remote Access – Privileged Commands and Access	CUI	3.1.12
AC-18	Wireless Access	CUI	3.1.16
AC-18(1)	Wireless Access – Authentication and Encryption	CUI	3.1.16
AC-18(3)	Wireless Access – Disable Wireless Networking	CUI	3.1.16
AC-19	Access Control for Mobile Devices	CUI	3.1.18
AC-19(5)	Access Control for Mobile Devices – Full Device or Container-Based Encryption	CUI	3.1.18
AC-20	Use of External Systems	CUI	3.1.20
AC-20(1)	Use of External Systems – Limits on Authorized Use	CUI	3.1.21
AC-20(2)	Use of External Systems – Portable Storage Devices – Restricted Use	CUI	3.1.21
AC-21	Information Sharing	FED	—
AC-22	Publicly Accessible Content	CUI	3.1.22

Table 4. Awareness and Training

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AT-1	Policy and Procedures	CUI	3.15.1
AT-2	Literacy Training and Awareness	CUI	3.2.1
AT-2(2)	Literacy Training and Awareness – Insider Threat	CUI	3.2.3
AT-2(3)	Literacy Training and Awareness – Social Engineering and Mining	CUI	3.2.3
AT-3	Role-Based Training	CUI	3.2.2
AT-4	Training Records	NCO	—

Table 5. Audit and Accountability

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AU-1	Policy and Procedures	CUI	3.15.1
AU-2	Event Logging	CUI	3.3.1
AU-3	Content of Audit Records	CUI	3.3.2
AU-3(1)	Additional Audit Information	CUI	3.3.2
AU-4	Audit Log Storage Capacity	NCO	—
AU-5	Response to Audit Logging Process Failures	CUI	3.3.4

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AU-6	Audit Record Review, Analysis, and Reporting	CUI	3.3.5
AU-6(1)	Audit Record Review, Analysis, and Reporting – Automated Process Integration	NCO	—
AU-6(3)	Audit Record Review, Analysis, and Reporting – Correlate Audit Record Repositories	CUI	3.3.5
AU-7	Audit Record Reduction and Report Generation	CUI	3.3.6
AU-7(1)	Audit Record Reduction and Report Generation – Automatic Processing	NCO	—
AU-8	Time Stamps	CUI	3.3.7
AU-9	Protection of Audit Information	CUI	3.3.8
AU-9(4)	Protection of Audit Information – Access by Subset of Privileged Users	CUI	3.3.9
AU-11	Audit Record Retention	CUI	3.3.3
AU-12	Audit Record Generation	CUI	3.3.3

Table 6. Assessment, Authorization, and Monitoring

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CA-1	Policy and Procedures	CUI	3.15.1
CA-2	Control Assessments	CUI	3.12.1
CA-2(1)	Control Assessments – Independent Assessors	CUI	3.12.5
CA-3	Information Exchange	CUI	3.12.6
CA-5	Plan of Action and Milestones	CUI	3.12.2
CA-6	Authorization	FED	—
CA-7	Continuous Monitoring	CUI	3.12.3
CA-7(1)	Continuous Monitoring – Independent Assessment	FED	—
CA-7(4)	Continuous Monitoring – Risk Monitoring	NCO	—
CA-9	Internal System Connections	CUI	3.12.7

Table 7. Configuration Management

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CM-1	Policy and Procedures	CUI	3.15.1
CM-2	Baseline Configuration	CUI	3.4.1
CM-2(2)	Baseline Configuration – Automation Support for Accuracy and Currency	NCO	—
CM-2(3)	Baseline Configuration – Retention of Previous Configurations	NCO	—
CM-2(7)	Baseline Configuration – Configure Systems and Components for High-Risk Areas	CUI	3.4.12
CM-3	Configuration Change Control	CUI	3.4.3
CM-3(2)	Configuration Change Control – Testing, Validation, and Documentation of Changes	NCO	—
CM-3(4)	Configuration Change Control – Security and Privacy Representatives	NCO	—
CM-4	Impact Analyses	CUI	3.4.4

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CM-4(2)	Impact Analyses – Verification of Controls	CUI	3.4.4
CM-5	Access Restrictions for Change	CUI	3.4.5
CM-6	Configuration Settings	CUI	3.4.2
CM-7	Least Functionality	CUI	3.4.6
CM-7(1)	Least Functionality – Periodic Review	CUI	3.4.6
CM-7(2)	Least Functionality – Prevent Program Execution	CUI	3.4.6
CM-7(5)	Least Functionality – Authorized Software – Allow by Exception	CUI	3.4.8
CM-8	System Component Inventory	CUI	3.4.10
CM-8(1)	System Component Inventory – Updates During Installation and Removal	CUI	3.4.10
CM-8(3)	System Component Inventory – Automated Unauthorized Component Detection	NCO	—
CM-9	Configuration Management Plan	NFO	—
CM-10	Software Usage Restrictions	NCO	—
CM-11	User-Installed Software	CUI	3.4.9
CM-12	Information Location	CUI	3.4.11
CM-12(1)	Information Location – Automated Tools to Support Information Location	NCO	—

Table 8. Contingency Planning

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CP-1	Policy and Procedures	NCO	—
CP-2	Contingency Plan	NCO	—
CP-2(1)	Contingency Plan – Coordinate with Related Plans	NCO	—
CP-2(3)	Contingency Plan – Resume Mission and Business Functions	NCO	—
CP-2(8)	Contingency Plan – Identify Critical Assets	NCO	—
CP-3	Contingency Training	NCO	—
CP-4	Contingency Plan Testing	NCO	—
CP-4(1)	Contingency Plan Testing – Coordinate Related Plans	NCO	—
CP-6	Alternate Storage Site	NCO	—
CP-6(1)	Alternate Storage Site – Separation of Primary Site	NCO	—
CP-6(3)	Alternate Storage Site – Accessibility	NCO	—
CP-7	Alternate Processing Site	NCO	—
CP-7(1)	Alternate Processing Site – Separation of Primary Site	NCO	—
CP-7(2)	Alternate Processing Site – Accessibility	NCO	—
CP-7(3)	Alternate Processing Site – Priority of Service	NCO	—
CP-8	Telecommunications Services	NCO	—
CP-8(1)	Telecommunications Services – Priority of Service Provisions	NCO	—
CP-8(2)	Telecommunications Services – Single Points of Failure	NCO	—
CP-9	System Backup	NCO	—
CP-9(1)	System Backup – Testing for Reliability and Integrity	NCO	—
CP-9(8)	System Backup – Cryptographic Protection	CUI	3.8.9
CP-10	System Recovery and Reconstitution	NCO	—
CP-10(2)	System Recovery and Reconstitution – Transaction Recovery	NCO	—

3024 **Table 9.** Identification and Authentication

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IA-1	Policy and Procedures	CUI	3.15.1
IA-2	Identification and Authentication (Organizational Users)	CUI	3.5.1
IA-2(1)	Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Privileged Accounts	CUI	3.5.3
IA-2(2)	Identification and Authentication (Organizational Users) – Multi-Factor Authentication to Non-Privileged Accounts	CUI	3.5.3
IA-2(8)	Identification and Authentication (Organizational Users) – Access to Accounts – Replay Resistant	CUI	3.5.4
IA-2(12)	Identification and Authentication (Organizational Users) – Acceptance of PIV Credentials	FED	—
IA-3	Device Identification and Authentication	CUI	3.5.2
IA-4	Identifier Management	CUI	3.5.5
IA-4(4)	Identifier Management – Identify User Status	CUI	3.5.5
IA-5	Authenticator Management	CUI	3.5.12
IA-5(1)	Authenticator Management – Password-Based Authentication	CUI	3.5.7
IA-5(2)	Authenticator Management – Public Key-Based Authentication	FED	—
IA-5(6)	Authenticator Management – Protection of Authenticators	CUI	3.5.12
IA-6	Authentication Feedback	CUI	3.5.11
IA-7	Cryptographic Module Authentication	FED	—
IA-8	Identification and Authentication (Non-Organizational Users)	FED	—
IA-8(1)	Identification and Authentication (Non-Organizational Users) – Acceptance of PIV Credentials from Other Agencies	FED	—
IA-8(2)	Identification and Authentication (Non-Organizational Users) – Acceptance of External Authenticators	FED	—
IA-8(4)	Identification and Authentication (Non-Organizational Users) – Use of Defined Profiles	FED	—
IA-11	Re-Authentication	CUI	3.5.1
IA-12	Identity Proofing	FED	—
IA-12(2)	Identity Proofing – Identity Evidence	FED	—
IA-12(3)	Identity Proofing – Identity Evidence Validation and Verification	FED	—
IA-12(5)	Identity Proofing – Address Confirmation	FED	—

3025

3026 **Table 10.** Incident Response

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IR-1	Policy and Procedures	CUI	3.15.1
IR-2	Incident Response Training	CUI	3.6.4
IR-3	Incident Response Testing	CUI	3.6.3
IR-3(2)	Incident Response Testing – Coordinate with Related Plans	NCO	—
IR-4	Incident Handling	CUI	3.6.1
IR-4(1)	Incident Handling – Automated Incident Handling Processes	NCO	—
IR-5	Incident Monitoring	CUI	3.6.2

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IR-6	Incident Reporting	CUI	3.6.2
IR-6(1)	Incident Reporting – Automated Reporting	NCO	—
IR-6(3)	Incident Reporting – Supply Chain Coordination	NCO	—
IR-7	Incident Response Assistance	CUI	3.6.2
IR-7(1)	Incident Response Assistance – Automation Support for Availability of Information and Support	NCO	—
IR-8	Incident Response Plan	CUI	3.6.1

Table 11. Maintenance

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MA-1	System Maintenance Policy and Procedures	CUI	3.15.1
MA-2	Controlled Maintenance	NCO	—
MA-3	Maintenance Tools	CUI	3.7.4
MA-3(1)	Maintenance Tools – Inspect Tools	CUI	3.7.4
MA-3(2)	Maintenance Tools – Inspect Media	CUI	3.7.4
MA-3(3)	Maintenance Tools – Prevent Unauthorized Removal	CUI	3.7.4
MA-4	Nonlocal Maintenance	CUI	3.7.5
MA-4(2)	Nonlocal Maintenance – Document Nonlocal Maintenance	NCO	—
MA-5	Maintenance Personnel	CUI	3.7.6
MA-6	Timely Maintenance	NCO	—

Table 12. Media Protection

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MP-1	Policy and Procedures	CUI	3.15.1
MP-2	Media Access	CUI	3.8.2
MP-3	Media Marking	CUI	3.8.4
MP-4	Media Storage	CUI	3.8.1
MP-5	Media Transport	CUI	3.8.5
MP-6	Media Sanitization	CUI	3.8.3
MP-7	Media Use	CUI	3.8.7

Table 13. Physical and Environmental Protection

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PE-1	Policy and Procedures	CUI	3.15.1
PE-2	Physical Access Authorizations	CUI	3.10.1

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PE-3	Physical Access Control	CUI	3.10.7
PE-4	Access Control for Transmission	CUI	3.10.8
PE-5	Access Control for Output Devices	CUI	3.10.8
PE-6	Monitoring Physical Access	CUI	3.10.2
PE-6(1)	Monitoring Physical Access – Intrusion Alarms and Surveillance Equipment	NCO	—
PE-8	Visitor Access Records	NFO	—
PE-9	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(1)	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	NFO	—
PE-17	Alternate Work Site	CUI	3.10.6

Table 14. Planning

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PL-1	Policy and Procedures	CUI	3.15.1
PL-2	System Security and Privacy Plans	CUI	3.15.2
PL-4	Rules of Behavior	CUI	3.15.3
PL-4(1)	Rules of Behavior – Social Media and External Site/Application Usage Restrictions	NCO	—
PL-8	Security and Privacy Architectures	NFO	—
PL-10	Baseline Selection	FED	—
PL-11	Baseline Tailoring	FED	—

Table 15. Program Management

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PM-1	Information Security Program Plan	NA	—
PM-2	Information Security Program Leadership Role	NA	—
PM-3	Information Security and Privacy Resources	NA	—
PM-4	Plan of Action and Milestones Process	NA	—
PM-5	System Inventory	NA	—
PM-5(1)	System Inventory – Inventory of Personally Identifiable Information	NA	—
PM-6	Measures of Performance	NA	—
PM-7	Enterprise Architecture	NA	—

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PM-7(1)	Enterprise Architecture – Offloading	NA	—
PM-8	Critical Infrastructure Plan	NA	—
PM-9	Risk Management Strategy	NA	—
PM-10	Authorization Process	NA	—
PM-11	Mission and Business Process Definition	NA	—
PM-12	Insider Threat Program	NA	—
PM-13	Security and Privacy Workforce	NA	—
PM-14	Testing, Training, and Monitoring	NA	—
PM-15	Security and Privacy Groups and Associations	NA	—
PM-16	Threat Awareness Program	NA	—
PM-16(1)	Threat Awareness Program – Automated Means for Sharing Threat Intelligence	NA	—
PM-17	Protecting Controlled Unclassified Information on External Systems	NA	—
PM-18	Privacy Program Plan	NA	—
PM-19	Privacy Program Leadership Role	NA	—
PM-20	Dissemination of Privacy Program Information	NA	—
PM-20(1)	Dissemination of Privacy Program Information – Privacy Policies on Websites, Applications, and Digital Services	NA	—
PM-21	Accounting of Disclosures	NA	—
PM-22	Personally Identifiable Information Quality Management	NA	—
PM-23	Data Governance Body	NA	—
PM-24	Data Integrity Board	NA	—
PM-25	Minimization of PII Used in Testing, Training, and Research	NA	—
PM-26	Complaint Management	NA	—
PM-27	Privacy Reporting	NA	—
PM-28	Risk Framing	NA	—
PM-29	Risk Management Program Leadership Roles	NA	—
PM-30	Supply Chain Risk Management Strategy	NA	—
PM-30(1)	Supply Chain Risk Management Strategy – Suppliers of Critical or Mission-Essential Items	NA	—
PM-31	Continuous Monitoring Strategy	NA	—
PM-32	Purposing	NA	—

Table 16. Personnel Security

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PS-1	Policy and Procedures	CUI	3.15.1
PS-2	Position Risk Designation	FED	—
PS-3	Personnel Screening	CUI	3.9.1
PS-4	Personnel Termination	CUI	3.9.2
PS-5	Personnel Transfer	CUI	3.9.2
PS-6	Access Agreements	NFO	—
PS-7	External Personnel Security	CUI	3.9.3

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PS-8	Personnel Sanctions	NCO	—
PS-9	Position Descriptions	FED	—

3039

3040 **Table 17.** PII Processing and Transparency

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PT-1	Policy and Procedures	NA	—
PT-2	Authority to Process Personally Identifiable Information	NA	—
PT-2(1)	Authority to Process Personally Identifiable Information – Data Tagging	NA	—
PT-2(2)	Authority to Process Personally Identifiable Information – Automation	NA	—
PT-3	Personally Identifiable Information Processing Purposes	NA	—
PT-3(1)	Personally Identifiable Information Processing Purposes – Data Tagging	NA	—
PT-3(2)	Personally Identifiable Information Processing Purposes – Automation	NA	—
PT-4	Consent	NA	—
PT-4(1)	Consent – Tailored Consent	NA	—
PT-4(2)	Consent – Just--in-Time Consent	NA	—
PT-4(3)	Consent – Revocation	NA	—
PT-5	Privacy Notice	NA	—
PT-5(1)	Privacy Notice – Just-in-Time Notice	NA	—
PT-5(2)	Privacy Notice – Privacy Act Statements	NA	—
PT-6	System of Records Notice	NA	—
PT-6(1)	System of Records Notice – Routine Uses	NA	—
PT-6(2)	System of Records Notice – Exemption Rules	NA	—
PT-7	Specific Categories of Personally Identifiable Information	NA	—
PT-7(1)	Specific Categories of Personally Identifiable Information – Social Security Numbers	NA	—
PT-7(2)	Specific Categories of Personally Identifiable Information – First Amendment Information	NA	—
PT-8	Computer Matching Requirements	NA	—

3041

3042 **Table 18.** Risk Assessment

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
RA-1	Policy and Procedures	CUI	3.15.1
RA-2	Security Categorization	FED	—
RA-3	Risk Assessment	CUI	3.11.1
RA-3(1)	Risk Assessment – Supply Chain Risk Assessment	CUI	3.11.1
RA-5	Vulnerability Monitoring and Scanning	CUI	3.11.2
RA-5(2)	Vulnerability Monitoring and Scanning – Update Vulnerabilities to be Scanned	CUI	3.11.2
RA-5(5)	Vulnerability Monitoring and Scanning – Privileged Access	CUI	3.11.2

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
RA-5(11)	Vulnerability Monitoring and Scanning – Public Disclosure Program	NCO	—
RA-7	Risk Response	CUI	3.11.4
RA-9	Criticality Analysis	NCO	—

3043

3044 **Table 19.** System and Services Acquisition

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SA-1	Policy and Procedures	CUI	3.15.1
SA-2	Allocation of Resources	NFO	—
SA-3	System Development Life Cycle	NFO	—
SA-4	Acquisition Process	NFO	—
SA-4(1)	Acquisition Process – Functional Properties of Controls	NFO	—
SA-4(2)	Acquisition Process – Design and Implementation Information for Controls	NFO	—
SA-4(9)	Acquisition Process – Functions, Ports, Protocols, and Services in Use	NFO	—
SA-4(10)	Acquisition Process – Use of Approved PIV Products	FED	—
SA-5	System Documentation	NFO	—
SA-8	Security and Privacy Engineering Principles	CUI	3.16.1
SA-9	External System Services	CUI	3.16.3
SA-9(2)	External System Services – Identification of Functions, Ports, Protocols, and Services	NCO	—
SA-10	Developer Configuration Management	NFO	—
SA-11	Developer Testing and Evaluation	NFO	—
SA-15	Development Process, Standards, and Tools	NFO	—
SA-15(3)	Development Process, Standards, and Tools – Criticality Analysis	NFO	—
SA-22	Unsupported System Components	CUI	3.16.2

3045

3046 **Table 20.** System and Communications Protection

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SC-1	Policy and Procedures	CUI	3.15.1
SC-2	Separation of System and User Functionality	CUI	3.13.3
SC-4	Information in Shared System Resources	CUI	3.13.4
SC-5	Denial-of-Service Protection	NCO	—
SC-7	Boundary Protection	CUI	3.13.1
SC-7(3)	Boundary Protection – Access Points	CUI	3.13.18
SC-7(4)	Boundary Protection – External Telecommunications Services	NFO	—
SC-7(5)	Boundary Protection – Deny by Default – Allow by Exception	CUI	3.13.6
SC-7(7)	Boundary Protection – Split Tunneling for Remote Devices	CUI	3.13.7
SC-7(8)	Boundary Protection – Route Traffic to Authenticated Proxy Servers	CUI	3.13.17
SC-8	Transmission Confidentiality and Integrity	CUI	3.13.8
SC-8(1)	Transmission Confidentiality and Integrity – Cryptographic Protection	CUI	3.13.8

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SC-10	Network Disconnect	CUI	3.13.9
SC-12	Cryptographic Key Establishment and Management	CUI	3.13.10
SC-13	Cryptographic Protection	CUI	3.13.11
SC-15	Collaborative Computing Devices and Applications	CUI	3.13.12
SC-17	Public Key Infrastructure Certificates	FED	—
SC-18	Mobile Code	CUI	3.13.13
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	3.13.15
SC-28	Protection of Information at Rest	CUI	3.13.8
SC-28(1)	Protection of Information at Rest – Cryptographic Protection	CUI	3.13.8
SC-39	Process Isolation	NFO	—

Table 21. System and Information Integrity

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SI-1	Policy and Procedures	CUI	3.15.1
SI-2	Flaw Remediation	CUI	3.14.1
SI-2(2)	Flaw Remediation – Automated Flaw Remediation Status	NCO	—
SI-3	Malicious Code Protection	CUI	3.14.2
SI-4	System Monitoring	CUI	3.14.6
SI-4(2)	System Monitoring – Automated Tools and Mechanisms for Real-Time Analysis	NCO	—
SI-4(4)	System Monitoring – Inbound and Outbound Communications Traffic	CUI	3.14.6
SI-4(5)	System Monitoring – System-Generated Alerts	NCO	—
SI-5	Security Alerts, Advisories, and Directives	CUI	3.14.3
SI-7	Software, Firmware, and Information Integrity	NCO	—
SI-7(1)	Software, Firmware, and Information Integrity – Integrity Checks	NCO	—
SI-7(7)	Software, Firmware, and Information Integrity – Integration of Detection and Response	NCO	—
SI-8	Spam Protection	CUI	3.14.8
SI-8(2)	Spam Protection – Automatic Updates	NCO	—
SI-10	Information Input Validation	NCO	—
SI-11	Error Handling	NCO	—
SI-12	Information Management and Retention	FED	—
SI-16	Memory Protection	NCO	—

3050 **Table 22.** Supply Chain Risk Management

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SR-1	Policy and Procedures	CUI	3.15.1
SR-2	Supply Chain Risk Management Plan	CUI	3.17.1
SR-2(1)	Supply Chain Risk Management Plan – Establish SCRM Team	NCO	—
SR-3	Supply Chain Controls and Processes	CUI	3.17.3
SR-5	Acquisition Strategies, Tools, and Methods	CUI	3.17.2
SR-6	Supplier Assessments and Reviews	CUI	3.11.1
SR-8	Notification Agreements	NCO	—
SR-10	Inspection of Systems or Components	NCO	—
SR-11	Component Authenticity	NCO	—
SR-11(1)	Component Authenticity – Anti-Counterfeit Training	NCO	—
SR-11(2)	Component Authenticity – Configuration Control for Component Service and Repair	NCO	—
SR-12	Component Disposal	CUI	3.17.4

3051

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 customer understanding
- Modified the security requirements and families in Section 3 to reflect the security controls in the NIST SP 800-53B [13] 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 (ODP) in selected security requirements to increase flexibility and help organizations better manage risk
- Grouped security requirements, where possible, to improve understanding and efficiency of implementation and assessments
- Removed outdated and redundant security requirements
- Added titles to security requirements
- Introduced a new tailoring category, *Not Applicable (NA)*
- Recategorized selected controls in the NIST SP 800-53B moderate baseline (using the tailoring criteria in Appendix C)
- Recast the security requirements, where possible, 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 table 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