



**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>

**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

1. Introduction	1
1.1. Purpose and Applicability	1
1.2. Organization of This Publication	2
2. The Fundamentals	3
2.1. Basic Assumptions	3
2.2. Security Requirement Development Methodology	3
3. The Requirements	5
3.1. Access Control	5
3.2. Awareness and Training	15
3.3. Audit and Accountability	17
3.4. Configuration Management	21
3.5. Identification and Authentication	27
3.6. Incident Response	31
3.7. Maintenance	33
3.8. Media Protection	35
3.9. Personnel Security	38
3.10. Physical Protection	39
3.11. Risk Assessment	42
3.12. Security Assessment and Monitoring	44
3.13. System and Communications Protection	47
3.14. System and Information Integrity	53
3.15. Planning	56
3.16. System and Services Acquisition	57
3.17. Supply Chain Risk Management	59
References	62
Appendix A. Acronyms	69
Appendix B. Glossary	72
Appendix C. Tailoring Criteria	79
Appendix D. Change Log	91

List of Tables

Table 1. Security requirement families	4
Table 2. Tailoring criteria and associated symbols.....	79
Table 3. Access Control.....	79
Table 4. Awareness and Training	80
Table 5. Audit and Accountability.....	80
Table 6. Assessment, Authorization, and Monitoring	81
Table 7. Configuration Management.....	81
Table 8. Contingency Planning	82
Table 9. Identification and Authentication	83
Table 10. Incident Response	83
Table 11. Maintenance	84
Table 12. Media Protection	84
Table 13. Physical and Environmental Protection	84
Table 14. Planning.....	85
Table 15. Program Management	85
Table 16. Personnel Security.....	86
Table 17. PII Processing and Transparency	87
Table 18. Risk Assessment	87
Table 19. System and Services Acquisition	88
Table 20. System and Communications Protection.....	88
Table 21. System and Information Integrity.....	89
Table 22. Supply Chain Risk Management	90
Table 23. Change Log	92

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 systems³ 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 requirements⁶ 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 agency⁸

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].

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

30 The security requirements in this publication are *only* applicable to components of nonfederal
31 systems⁹ that process, store, or transmit CUI *or* that provide protection for such components.¹⁰
32 The requirements are intended for use by federal agencies in contractual vehicles or other
33 agreements that are established between those agencies and nonfederal organizations.

34 **1.2. Organization of This Publication**

35 The remainder of this special publication is organized as follows:

- 36 • [Section 2](#) describes the assumptions and methodology used to develop the security
37 requirements for protecting the confidentiality of CUI; the format of the requirements;
38 and the tailoring criteria applied to the NIST standards and guidelines to obtain the
39 requirements.
- 40 • [Section 3](#) lists the security requirements for protecting the confidentiality of CUI in
41 nonfederal systems and organizations.

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

- 44 • [References](#)
- 45 • [Appendix A](#): Acronyms
- 46 • [Appendix B](#): Glossary
- 47 • [Appendix C](#): Tailoring Criteria
- 48 • [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.

49 **2. The Fundamentals**

50 This section describes the basic assumptions and methodology used to develop the requirements
51 to protect the confidentiality of CUI in nonfederal systems and organizations. It also includes the
52 tailoring¹¹ criteria applied to the requirements and controls in FIPS 200 [7] and NIST SP 800-53
53 [8].

54 **2.1. Basic Assumptions**

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

- 57 • Federal information designated as CUI has the same value, whether such information
58 resides in a federal or a nonfederal system or organization.
- 59 • Statutory and regulatory requirements for the protection of CUI are consistent in federal
60 and nonfederal systems and organizations.
- 61 • Safeguards implemented to protect CUI are consistent in federal and nonfederal systems
62 and organizations.
- 63 • The confidentiality impact value for CUI is no less than *moderate*.¹²

64 **2.2. Security Requirement Development Methodology**

65 Starting with the NIST SP 800-53 security controls in the NIST SP 800-53B [13] moderate
66 control baseline, which satisfy the minimum-security requirements in FIPS 200, the controls are
67 tailored to eliminate selected controls or parts of controls that are:

- 68 • Primarily the responsibility of the Federal Government
- 69 • Not directly related to protecting the confidentiality of CUI
- 70 • Expected to be implemented by nonfederal organizations without specification by the
71 Federal Government

72 The NIST SP 800-171 security requirements represent a subset of the controls that are necessary
73 for a comprehensive information security program. The security requirements are organized into
74 17 families, as illustrated in [Table 1](#). Each family contains the particular requirements related to
75 the general security topic of the family. Certain families from NIST SP 800-53 are not included
76 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.

111 3. The Requirements

112 This section describes 17 families of security requirements for protecting the confidentiality of
113 CUI in nonfederal systems and organizations. When used in the context of the requirements in
114 Section 3, the term *system* means a nonfederal system that processes, stores, or transmits CUI.

115 3.1. Access Control

116 3.1.1. Account Management

- 117 a. Define and document the types of system accounts allowed and prohibited.
- 118 b. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment:*
119 *organization-defined policy, procedures, prerequisites, and criteria*].
- 120 c. Specify authorized users of the system, group and role membership, and access
121 authorizations (i.e., privileges).
- 122 d. Authorize access to the system based on a valid access authorization and intended system
123 usage.
- 124 e. Monitor the use of accounts.
- 125 f. Disable accounts of individuals within [*Assignment: organization-defined time period*] when
126 the accounts:
 - 127 1. Have expired;
 - 128 2. Are no longer associated with a user or individual;
 - 129 3. Are in violation of organizational policy; or
 - 130 4. Have been inactive for [*Assignment: organization-defined time period*].
- 131 g. Disable accounts of individuals within [*Assignment: organization-defined time period*] of
132 discovery of [*Assignment: organization-defined significant risks*].
- 133 h. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment:*
134 *organization-defined time period*]:
 - 135 1. When accounts are no longer required;
 - 136 2. When users are terminated or transferred; and
 - 137 3. When system usage or need-to-know changes for an individual.

138 DISCUSSION

139 This requirement focuses on account management for systems and applications. The definition of
140 and enforcement of access authorizations other than those determined by account type (e.g.,
141 privileged access, non-privileged access) are addressed in requirement 3.1.2. System account
142 types include individual, shared, group, temporary, system, guest, anonymous, emergency,
143 developer, and service. Users who require administrative privileges on system accounts receive
144 additional scrutiny by organizational personnel responsible for approving such accounts and
145 privileged access. Types of accounts that organizations may prohibit due to increased risk include
146 shared, group, emergency, guest, anonymous, and temporary.

147 Organizations may choose to define access privileges or other attributes by account, by type of
148 account, or a combination of both. Other attributes required for authorizing access include
149 restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes,

150 organizations consider system-related requirements (e.g., system upgrades, scheduled
151 maintenance) and mission and business requirements (e.g., time zone differences, remote access
152 to support travel requirements).

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

159 REFERENCES

160 Source Controls: [AC-2](#), [AC-2\(3\)](#), [AC-2\(13\)](#)
161 Supporting Publications: SP 800-46 [15], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18],
162 SP 800-77 [19], SP 800-113 [20], SP 800-114 [21], SP 800-121 [22], SP 800-162 [23], SP 800-
163 178 [24], SP 800-192 [25], IR 7874 [26], IR 7966 [27]

164 3.1.2. Access Enforcement

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

167 DISCUSSION

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

175 REFERENCES

176 Source Controls: [AC-3](#), [AC-17](#)
177 Supporting Publications: SP 800-46 [15], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18],
178 SP 800-77 [19], SP 800-113 [20], SP 800-114 [21], SP 800-121 [22], SP 800-162 [23], SP 800-
179 178 [24], SP 800-192 [25], IR 7874 [26], IR 7966 [27]

180 3.1.3. Flow Enforcement

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

183 DISCUSSION

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

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

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

210 REFERENCES

211 Source Controls: [AC-4](#)
212 Supporting Publications: SP 800-160-1 [12], SP 800-162 [23], SP 800-178 [24]

213 3.1.4. Separation of Duties

- 214 a. Identify the duties of individuals requiring separation.
- 215 b. Define system access authorizations to support separation of duties.

216 DISCUSSION

217 Separation of duties addresses the potential for abuse of authorized privileges and helps reduce
218 the risk of malevolent activity without collusion. Separation of duties includes dividing mission
219 functions and support functions among different individuals or roles, conducting system support
220 functions with different individuals or roles (e.g., quality assurance, configuration management,
221 testing, system management, programming, and network security), and ensuring that security
222 personnel who administer access control functions do not also administer audit functions.
223 Because separation of duty violations can span systems and application domains, organizations
224 consider the entirety of their systems and system components when developing policies on
225 separation of duties.

226 REFERENCES

227 Source Controls: [AC-5](#)
228 Supporting Publications: SP 800-162 [23], SP 800-178 [24]

229 3.1.5. Least Privilege

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

- 232 b. Authorize access for [Assignment: organization-defined individuals or roles] to [Assignment:
233 organization-defined security functions and security-relevant information].
- 234 c. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment:
235 organization-defined roles or classes of users] to validate the need for such privileges.
- 236 d. Reassign or remove privileges, as necessary.

237 **DISCUSSION**

238 Organizations employ the principle of least privilege for specific duties and authorized access for
239 users and processes. Security functions include establishing system accounts, configuring access
240 authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and
241 establishing intrusion detection parameters. Security-relevant information includes filtering rules
242 for routers or firewalls, configuration parameters for security services, cryptographic key
243 management information, and access control lists. Authorized personnel include security
244 administrators, system administrators, system security officers, system programmers, and other
245 privileged users. Organizations consider creating additional processes, roles, and system accounts
246 to achieve least privilege. Least privilege is also applied to the development, implementation, and
247 operation of the system.

248 **REFERENCES**

249 Source Controls: [AC-6](#), [AC-6\(1\)](#), [AC-6\(7\)](#)
250 Supporting Publications: None

251 **3.1.6. Least Privilege – Privileged Accounts**

- 252 a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or
253 roles].
- 254 b. Require that users of system accounts (or roles) with access to [Assignment: organization-
255 organization-defined security functions or security-relevant information] use non-privileged accounts or
256 roles when accessing nonsecurity functions.

257 **DISCUSSION**

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

265 Requiring the use of non-privileged accounts when accessing nonsecurity functions limits
266 exposure when operating from within privileged accounts or roles. The inclusion of roles
267 addresses situations in which organizations implement access control policies, such as role-based
268 access control, and where a change of role provides the same degree of assurance in the change of
269 access authorizations for the user and the processes acting on behalf of the user as would be
270 provided by a change between a privileged and non-privileged account.

271 **REFERENCES**

272 Source Controls: [AC-6\(2\)](#), [AC-6\(5\)](#)
273 Supporting Publications: None

274 3.1.7. Least Privilege – Privileged Functions

- 275 a. Prevent non-privileged users from executing privileged functions.
- 276 b. Log the execution of privileged functions.

277 DISCUSSION

278 Privileged functions include establishing system accounts, performing system integrity checks,
279 conducting patching operations, or administering cryptographic key management activities. Non-
280 privileged users do not possess appropriate authorizations. Circumventing intrusion detection and
281 prevention mechanisms or malicious code protection mechanisms are examples of privileged
282 functions that require protection from non-privileged users. Note that this requirement represents
283 a condition to be achieved by the definition of authorized privileges in 3.1.2.

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

289 REFERENCES

290 Source Controls: [AC-6\(9\)](#), [AC-6\(10\)](#)
291 Supporting Publications: None

292 3.1.8. Unsuccessful Logon Attempts

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

295 DISCUSSION

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

301 REFERENCES

302 Source Controls: [AC-7](#)
303 Supporting Publications: SP 800-63-3 [28], SP 800-124 [29]

304 3.1.9. System Use Notification

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

307 DISCUSSION

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

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

316 REFERENCES

317 Source Controls: [AC-8](#)

318 Supporting Publications: None

319 3.1.10. Device Lock

- 320 a. Prevent access to the system by [*Selection (one or more): initiating a device lock after*
321 [*Assignment: organization-defined time period*] of inactivity; requiring the user to initiate a
322 device lock before leaving the system unattended].
- 323 b. Retain the device lock until the user reestablishes access using established identification
324 and authentication procedures.
- 325 c. Conceal, via the device lock, information previously visible on the display with a publicly
326 viewable image.

327 DISCUSSION

328 Device locks are temporary actions taken to prevent access to the system when users depart
329 from the immediate vicinity of the system but do not want to log out because of the temporary
330 nature of their absences. Device locks can be implemented at the operating system or
331 application level. User-initiated device locking is behavior- or policy-based and requires users
332 to take physical action to initiate the device lock. Device locks are not an acceptable substitute
333 for logging out of the system, such as when organizations require users to log out at the end of
334 workdays. Pattern-hiding displays can include static or dynamic images, such as patterns used
335 with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank
336 screen with the caveat that controlled unclassified information is not displayed.

337 REFERENCES

338 Source Controls: [AC-11](#), [AC-11\(1\)](#)

339 Supporting Publications: None

340 3.1.11. Session Termination

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

343 DISCUSSION

344 This requirement addresses the termination of user-initiated logical sessions in contrast to the
345 termination of network connections that are associated with communications sessions (i.e.,
346 disconnecting from the network) in 3.13.9. A logical session is initiated whenever a user (or
347 process acting on behalf of a user) accesses a system. Such sessions can be terminated (and
348 terminate user access) without terminating network sessions. Session termination terminates all
349 processes associated with a user's logical session except those processes that are specifically
350 created by the user (i.e., session owner) to continue after the session is terminated. Conditions
351 or trigger events that require automatic session termination can include organization-defined
352 periods of user inactivity, time-of-day restrictions on system use, and targeted responses to
353 certain types of incidents.

354 **REFERENCES**

355 Source Controls: [AC-12](#)
356 Supporting Publications: None

357 **3.1.12. Remote Access**

- 358 a. Establish, authorize, and document usage restrictions, configurations, and connections
359 allowed for each type of permitted remote access.
- 360 b. Monitor and control remote access methods.
- 361 c. Route remote access to the system through managed access control points.
- 362 d. Authorize remote execution of privileged commands and remote access to security-relevant
363 information.
- 364 e. Implement cryptographic mechanisms to protect the confidentiality of remote access
365 sessions.

366 **DISCUSSION**

367 Remote access to the system represents a significant potential vulnerability that can be exploited
368 by adversaries. Monitoring and controlling remote access methods allows organizations to
369 detect attacks and help ensure compliance with remote access policies. This occurs by auditing
370 the connection activities of remote users on a variety of systems, including servers, notebook
371 computers, workstations, smart phones, and tablets. Routing remote access through managed
372 access control points enhances explicit control over such connections. It also reduces the
373 susceptibility to unauthorized access to the system which could result in the unauthorized
374 disclosure of CUI.

375 Restricting the execution of privileged commands and access to security-relevant information
376 via remote access reduces the exposure of the organization and its susceptibility to threats by
377 adversaries. A privileged command is a human-initiated command executed on a system that
378 involves the control, monitoring, or administration of the system, including security functions
379 and security-relevant information. Security-relevant information is information that can
380 potentially impact the operation of security functions or the provision of security services in a
381 manner that could result in failure to enforce the system security policy or maintain isolation of
382 code and data. Privileged commands give individuals the ability to execute sensitive, security-
383 critical, or security-relevant system functions. Controlling access from remote locations helps to
384 ensure that unauthorized individuals are not able to execute such commands with the potential
385 to do serious or catastrophic damage to the system.

386 **REFERENCES**

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

390 **3.1.13.** Withdrawn: Incorporated into 3.1.12.

391 **3.1.14.** Withdrawn: Incorporated into 3.1.12.

392 **3.1.15.** Withdrawn: Incorporated into 3.1.12.

393 **3.1.16. Wireless Access**

- 394 a. Establish configuration requirements, connection requirements, and implementation
395 guidance for wireless access to the system.
- 396 b. Authorize wireless access to the system prior to allowing such connections.
- 397 c. Protect wireless access to the system using authentication and encryption.
- 398 d. Disable, when not intended for use, wireless networking capabilities embedded within the
399 system prior to issuance and deployment.

400 **DISCUSSION**

401 Establishing usage restrictions, configuration requirements, and connection requirements for
402 wireless access to the system provides criteria for organizations to support wireless access
403 authorization decisions. These restrictions and requirements help to reduce the susceptibility to
404 unauthorized system access through wireless technologies. Wireless networks use
405 authentication protocols that provide credential protection and mutual authentication.
406 Organizations authenticate individuals and devices to protect wireless access to the system.
407 Special attention is given to the wide variety of devices that are part of the Internet of Things
408 with potential wireless access to the system. Wireless networking capabilities that are embedded
409 within system components represent a significant potential vulnerability that can be exploited
410 by adversaries. Disabling wireless capabilities when not needed for essential organizational
411 missions or functions can reduce susceptibility to threats by adversaries involving wireless
412 technologies.

413 **REFERENCES**

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

416 **3.1.17.** Withdrawn: Incorporated into 3.1.16.

417 **3.1.18. Access Control for Mobile Devices**

- 418 a. Establish configuration requirements, connection requirements, and implementation
419 guidance for organization-controlled mobile devices.
- 420 b. Authorize the connection of mobile devices to the system.
- 421 c. Implement [*Selection: full-device encryption; container-based encryption*] to protect the
422 confidentiality of CUI on mobile devices.

423 **DISCUSSION**

424 A mobile device is a computing device that has a small form factor such that it can easily be
425 carried by a single individual; is designed to operate without a physical connection; possesses
426 local, non-removable or removable data storage; and includes a self-contained power source.
427 Mobile device functionality may also include voice communication capabilities, on-board
428 sensors that allow the device to capture information, and/or built-in features for synchronizing
429 local data with remote locations. Examples include smart phones and tablets. Mobile devices
430 are typically associated with a single individual. The processing, storage, and transmission
431 capability of mobile devices may be comparable to or a subset of notebook/desktop systems,
432 depending on the nature and intended purpose of the device. The protection and control of
433 mobile devices is behavior- or policy-based and requires users to take physical action to protect

434 and control such devices when outside of controlled areas. Controlled areas are spaces for
435 which the organization provides physical or procedural controls to meet the requirements
436 established for protecting CUI.

437 Due to the large variety of mobile devices with different characteristics and capabilities,
438 organizational restrictions may vary for the different classes or types of such devices. Usage
439 restrictions and specific implementation guidance for mobile devices include configuration
440 management, device identification and authentication, implementation of mandatory protective
441 software, scanning devices for malicious code, updating virus protection software, scanning for
442 critical software updates and patches, conducting primary operating system (and possibly other
443 resident software) integrity checks, and disabling unnecessary hardware.

444 Organizations can employ full-device encryption or container-based encryption to protect the
445 confidentiality of CUI on mobile devices and computing platforms. Container-based encryption
446 provides a fine-grained approach to the encryption of data and information, including
447 encrypting selected data structures such as files, records, or fields.

448 **REFERENCES**

449 Source Controls: [AC-19](#), [AC-19\(5\)](#)

450 Supporting Publications: SP 800-114 [35], SP 800-124 [29]

451 **3.1.19.** Withdrawn: Incorporated into 3.1.18.

452 **3.1.20. Use of External Systems**

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

- 458 1. Access the system from external systems; and
- 459 2. Process, store, or transmit CUI using external systems; or

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

461 **DISCUSSION**

462 External systems are systems that are used by but are not part of the organizational system and
463 for which the organization has no direct control over the implementation of required controls or
464 the assessment of control effectiveness. External systems include personally owned systems,
465 system components, or devices; privately owned computing and communication devices in
466 commercial or public facilities; systems owned or controlled by nonfederal organizations; and
467 systems managed by contractors. Organizations have the option to prohibit the use of any type
468 of external system or specified types of external systems, (e.g., prohibit the use of any external
469 system that is not organizationally owned or prohibit the use of personally owned systems).

470 Authorized individuals include organizational personnel, contractors, or other individuals with
471 authorized access to the organizational system and over whom organizations have the authority
472 to impose specific rules of behavior regarding system access. Restrictions that organizations
473 impose on authorized individuals need not be uniform, as the restrictions may vary depending
474 on the trust relationships between organizations.

475 **REFERENCES**

476 Source Controls: [AC-20](#)
477 Supporting Publications: None

478 **3.1.21. External Systems – Limits and Restrictions on Authorized Use**

- 479 a. Permit authorized individuals to use an external system to access the system or to process,
480 store, or transmit CUI only after:
- 481 1. Implemented controls on the external system as specified in the organization’s security
482 policies and security plans are verified; or
 - 483 2. Approved system connection or processing agreements with the organizational entity
484 hosting the external system are retained.
- 485 b. Restrict the use of organization-controlled portable storage devices by authorized
486 individuals on external systems as follows: [*Assignment: organization-defined usage*
487 *restrictions*].

488 **DISCUSSION**

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

497 **REFERENCES**

498 Source Controls: [AC-20\(1\)](#), [AC-20\(2\)](#)
499 Supporting Publications: None

500 **3.1.22. Publicly Accessible Content**

- 501 a. Train authorized individuals to ensure that publicly accessible information does not contain
502 CUI.
- 503 b. Review the content on publicly accessible systems for CUI [*Assignment: organization-*
504 *defined frequency*] and remove such information, if discovered.

505 **DISCUSSION**

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

509 **REFERENCES**

510 Source Controls: [AC-22](#)
511 Supporting Publications: None

512 3.1.23. Account Management – Inactivity Logout

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

516 **DISCUSSION**

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

520 **REFERENCES**

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

523 3.2. Awareness and Training

524 3.2.1. Literacy Training and Awareness

- 525 a. Provide security literacy training to system users:
- 526 1. As part of initial training for new users and [*Assignment: organization-defined frequency*]
527 thereafter; and
 - 528 2. When required by system changes or following [*Assignment: organization-defined*
529 *events*].
- 530 b. Update training and awareness content [*Assignment: organization-defined frequency*] and
531 following [*Assignment: organization-defined events*].

532 **DISCUSSION**

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

541 Awareness techniques include displaying posters, offering supplies inscribed with security
542 reminders, displaying logon screen messages, generating email advisories or notices from
543 organizational officials, and conducting awareness events. Literacy training is conducted at a
544 frequency consistent with applicable laws, directives, regulations, and policies. Updating literacy
545 training and awareness content on a regular basis helps to ensure that the content remains
546 relevant. Events that may precipitate an update to literacy training and awareness content include,
547 but are not limited to, assessment or audit findings, security incidents or breaches, or changes in
548 applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

549 **REFERENCES**

550 Source Controls: [AT-2](#)
551 Supporting Publications: SP 800-50 [36]

552 3.2.2. Role-Based Training

- 553 a. Provide role-based security training to organizational personnel:
- 554 1. Before authorizing access to the system, CUI, or performing assigned duties, and
- 555 [Assignment: organization-defined frequency] thereafter; and
- 556 2. When required by system changes.
- 557 b. Update role-based training content [Assignment: organization-defined frequency] and
- 558 following [Assignment: organization-defined events].

559 DISCUSSION

560 Organizations determine the content and frequency of security training based on the assigned

561 duties, roles, and responsibilities of individuals and the security requirements of organizations

562 and the systems to which personnel have authorized access. In addition, organizations provide

563 system developers, enterprise architects, security architects, acquisition/procurement officials,

564 software developers, system developers, systems integrators, system and network administrators,

565 personnel conducting configuration management and auditing activities, personnel performing

566 independent verification and validation, security assessors, and personnel with access to system-

567 level software with security-related technical training specifically tailored for their assigned

568 duties.

569 Comprehensive role-based training addresses management, operational, and technical roles and

570 responsibilities that cover physical, personnel, and technical controls. Such training can include

571 policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide

572 the training necessary for individuals to carry out their responsibilities related to operations and

573 supply chain security within the context of organizational information security programs.

574 REFERENCES

575 Source Controls: [AT-3](#)

576 Supporting Publications: SP 800-161 [37], SP 800-181 [38]

577 3.2.3. Advanced Literacy Training

578 Provide literacy training on recognizing and reporting potential and actual indicators of insider

579 threat, social engineering, and social mining.

580 DISCUSSION

581 Potential indicators and possible precursors of insider threat include behaviors such as inordinate,

582 long-term job dissatisfaction; attempts to gain access to information that is not required for job

583 performance; unexplained access to financial resources; bullying or sexual harassment of fellow

584 employees; workplace violence; and other serious violations of the policies, procedures,

585 directives, rules, or practices of organizations. Security awareness training includes how to

586 communicate employee and management concerns regarding potential indicators of insider threat

587 through appropriate organizational channels in accordance with established organizational

588 policies and procedures. Organizations may consider tailoring insider threat awareness topics to

589 the role (e.g., training for managers may be focused on specific changes in the behavior of team

590 members, while training for employees may be focused on more general observations).

591 Social engineering is an attempt to deceive an individual into revealing information or taking an

592 action that can be used to breach, compromise, or otherwise adversely impact a system. Social

593 engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking,

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

599 REFERENCES

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

602 3.3. Audit and Accountability

603 3.3.1. Event Logging

- 604 a. Specify the following event types for logging within the system: [*Assignment: organization-*
605 *defined event types*].
- 606 b. Review and update the event types selected for logging [*Assignment: organization-defined*
607 *frequency*].

608 DISCUSSION

609 An event is any observable occurrence in a system, which includes unlawful or unauthorized
610 system activity. Organizations identify event types for which a logging functionality is needed as
611 those events that are significant and relevant to the security of systems and the environments in
612 which those systems operate to meet specific and ongoing auditing needs. Event types can
613 include password changes, failed logons or failed accesses related to systems, administrative
614 privilege usage, or third-party credential usage. In determining event types that require logging,
615 organizations consider the system monitoring and auditing that are appropriate for each of the
616 CUI security requirements. When defining event types, organizations consider the logging
617 necessary to cover related events, such as the steps in distributed, transaction-based processes
618 (e.g., processes that are distributed across multiple organizations) and actions that occur in
619 service-oriented or cloud-based architectures. Monitoring and auditing requirements can be
620 balanced with other system needs. For example, organizations may determine that systems must
621 have the capability to log every file access, both successful and unsuccessful, but not activate that
622 capability except for specific circumstances due to the potential burden on system performance.
623 The event types that are logged by organizations may change over time. Periodically reviewing
624 and updating the set of logged event types is necessary to ensure that the current set remains
625 necessary and sufficient.

626 REFERENCES

627 Source Controls: [AU-2](#)
628 Supporting Publications: SP 800-92 [39]

629 3.3.2. Audit Record Content

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

633 **DISCUSSION**

634 Audit record content that may be necessary to support the auditing function includes time stamps,
635 source and destination addresses, user or process identifiers, event descriptions, filenames, and
636 the access control or flow control rules that are invoked. Event outcomes can include indicators of
637 event success or failure and event-specific results (e.g., the security state of the system after the
638 event occurred). Detailed information that organizations may consider in audit records includes a
639 full text recording of privileged commands or the individual identities of group account users.

640 **REFERENCES**

641 Source Controls: [AU-3](#), [AU-3\(1\)](#)
642 Supporting Publications: None

643 **3.3.3. Audit Record Generation**

- 644 a. Provide an audit record generation capability for the event types defined in 3.3.1a.
645 b. Generate audit records for the event types defined in 3.3.1a. that include the audit record
646 content defined in 3.3.2.
647 c. Retain audit records for [*Assignment: organization-defined time period consistent with*
648 *records retention policy, applicable contract requirement, law, or regulation*].

649 **DISCUSSION**

650 Audit records can be generated at various levels of abstraction, including at the packet level as
651 information traverses the network. Selecting the appropriate level of abstraction is a critical
652 aspect of an audit logging capability and can facilitate the identification of root causes to
653 problems. The ability to add information generated in audit records is dependent on system
654 functionality to configure the audit record content. Organizations may consider additional
655 information in audit records including access control or flow control rules invoked and individual
656 identities of group account users. Organizations may also consider limiting additional audit
657 record information to only information that is explicitly needed for audit requirements.

658 **REFERENCES**

659 Source Controls: [AU-11](#), [AU-12](#)
660 Supporting Publications: SP 800-92 [39]

661 **3.3.4. Response to Audit Logging Process Failures**

- 662 a. Alert [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-*
663 *defined time period*] in the event of an audit logging process failure.
664 b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

665 **DISCUSSION**

666 Audit logging process failures include software and hardware errors, failures in audit log
667 capturing mechanisms, and reaching or exceeding audit log storage capacity. Response actions
668 include overwriting the oldest audit records, shutting down the system, and stopping the
669 generation of audit records. Organizations may choose to define additional actions for audit
670 logging process failures based on the type of failure, the location of the failure, the severity of the
671 failure, or a combination of such factors. When the audit logging process failure is related to
672 storage, the response is carried out for the audit log storage repository (i.e., the distinct system

673 component where the audit logs are stored), the system on which the audit logs reside, the total
674 audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or
675 all three. Organizations may decide to take no additional actions after alerting designated roles or
676 personnel.

677 REFERENCES

678 Source Controls: [AU-5](#)

679 Supporting Publications: None

680 3.3.5. Audit Record Review, Analysis, and Reporting

- 681 a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for
682 indications and potential impact of inappropriate or unusual activity.
- 683 b. Report findings to [*Assignment: organization-defined personnel or roles*].
- 684 c. Analyze and correlate audit records across different repositories to gain organization-wide
685 situational awareness.

686 DISCUSSION

687 Audit record review, analysis, and reporting covers information security-related logging
688 performed by organizations and can include logging that results from the monitoring of account
689 usage, remote access, wireless connectivity, configuration settings, the use of maintenance tools
690 and non-local maintenance, system component inventory, mobile device connection, physical
691 access, temperature and humidity, equipment delivery and removal, communications at system
692 interfaces, and the use of mobile code. Findings can be reported to organizational entities that
693 include the incident response team, help desk, and security or privacy offices. If organizations are
694 prohibited from reviewing and analyzing audit records or unable to conduct such activities, the
695 review or analysis may be carried out by other organizations granted such authority. The scope,
696 frequency, and/or depth of the audit record review, analysis, and reporting may be adjusted to
697 meet organizational needs based on new information received. Correlating audit record review,
698 analysis, and reporting processes helps to ensure that they do not operate independently but rather
699 collectively create a more complete view of events. Regarding the assessment of a given system,
700 the requirement is agnostic as to whether this correlation is applied at the system level or at the
701 organization level across all systems.

702 REFERENCES

703 Source Controls: [AU-6\(3\)](#)

704 Supporting Publications: SP 800-86 [40], SP 800-101 [41]

705 3.3.6. Audit Record Reduction and Report Generation

- 706 a. Implement an audit record reduction and report generation capability that supports on-
707 demand audit record review, analysis, reporting requirements, and after-the-fact
708 investigations of incidents.
- 709 b. Preserve the original content and time ordering of audit records.

710 DISCUSSION

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

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

719 **REFERENCES**

720 Source Controls: [AU-7](#)

721 Supporting Publications: None

722 **3.3.7. Time Stamps**

- 723 a. Use internal system clocks to generate time stamps for audit records.
- 724 b. Record time stamps for audit records that meet [*Assignment: organization-defined granularity*
725 *of time measurement*] and that:
- 726 1. Use Coordinated Universal Time (UTC);
 - 727 2. Have a fixed local time offset from UTC; or
 - 728 3. Include the local time offset as part of the time stamp.

729 **DISCUSSION**

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

738 **REFERENCES**

739 Source Controls: [AU-8](#), [SC-45](#), [SC-45\(1\)](#)

740 Supporting Publications: None

741 **3.3.8. Protection of Audit Information**

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

744 **DISCUSSION**

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

751 **REFERENCES**

752 Source Controls: [AU-9](#)

753 Supporting Publications: None

754 3.3.9. Audit Information Access

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

757 DISCUSSION

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

762 REFERENCES

763 Source Controls: [AU-9\(4\)](#)

764 Supporting Publications: None

765 3.4. Configuration Management

766 3.4.1. Baseline Configuration

- 767 a. Develop, document, and maintain under configuration control, a current baseline
768 configuration of the system.
- 769 b. Review and update the baseline configuration of the system [*Assignment: organization-*
770 *defined frequency*] and when system components are installed or upgraded.

771 DISCUSSION

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

780 REFERENCES

781 Source Controls: [CM-2](#)

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

783 3.4.2. Configuration Settings

- 784 a. Establish, document, and implement configuration settings for the system that reflect the
785 most restrictive mode consistent with operational requirements using [*Assignment:*
786 *organization-defined common secure configurations*].
- 787 b. Identify, document, and approve any deviations from established configuration settings.
- 788 c. Monitor and control changes to the configuration settings in accordance with organizational
789 policies and procedures.

790 **DISCUSSION**

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

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

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

811 **REFERENCES**

812 Source Controls: [CM-6](#)
813 Supporting Publications: SP 800-70 [48], SP 800-126 [49], SP 800-128 [45]

814 **3.4.3. Configuration Change Control**

- 815 a. Determine the types of changes to the system that are configuration-controlled.
816 b. Review proposed configuration-controlled changes to the system, and approve or disapprove
817 such changes with explicit consideration for security impacts.
818 c. Implement and document approved configuration-controlled changes to the system.
819 d. Monitor and review activities associated with configuration-controlled changes to the system.

820 **DISCUSSION**

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

828 **REFERENCES**

829 Source Controls: [CM-3](#)
830 Supporting Publications: SP 800-124 [29], SP 800-128 [45]

831 **3.4.4. Impact Analyses**

- 832 a. Analyze the security impact of changes to the system prior to implementation.
- 833 b. After system changes, verify that the impacted controls are implemented correctly, operating
- 834 as intended, and producing the desired outcome with regard to meeting specified security
- 835 requirements.

836 **DISCUSSION**

837 Organizational personnel with security responsibilities conduct impact analyses which include

838 reviewing security plans, policies, and procedures to understand security controls; reviewing

839 system design documentation and operational procedures to understand control implementation

840 and how specific system changes might affect the controls; reviewing with stakeholders, the

841 impact of changes on supply chain partners; and determining how potential changes to a system

842 create new risks and the ability of implemented controls to mitigate those risks. Impact analyses

843 also include risk assessments to understand the impact of changes and to determine whether

844 additional controls are required.

845 **REFERENCES**

846 Source Controls: [CM-4](#), [CM-4\(2\)](#)

847 Supporting Publications: SP 800-128 [45]

848 **3.4.5. Access Restrictions for Change**

849 Define, document, approve, and enforce physical and logical access restrictions associated with

850 changes to the system.

851 **DISCUSSION**

852 Changes to the hardware, software, or firmware components of systems or the operational

853 procedures related to the systems can have potentially significant effects on the security of the

854 systems. Therefore, organizations permit only qualified and authorized individuals to access

855 systems for the purpose of initiating changes. Access restrictions include physical and logical

856 access controls, software libraries, workflow automation, media libraries, abstract layers (i.e.,

857 changes implemented into external interfaces rather than directly into systems), and change

858 windows (i.e., changes occur only during specified times).

859 **REFERENCES**

860 Source Controls: [CM-5](#)

861 Supporting Publications: FIPS 140-3 [42], FIPS 180-4 [43], SP 800-128 [45]

862 **3.4.6. Least Functionality**

- 863 a. Configure the system to provide only mission-essential capabilities.
- 864 b. Prohibit or restrict use of the following functions, ports, protocols, software, and/or services:
- 865 *[Assignment: organization-defined prohibited or restricted functions, system ports, protocols,*
- 866 *software, and/or services].*
- 867 c. Prevent program execution in accordance with *[Selection (one or more): [Assignment:*
- 868 *organization-defined policies, rules of behavior, and/or access agreements regarding*
- 869 *software program usage and restrictions]; rules authorizing the terms and conditions of*
- 870 *software program usage].*

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

873 **DISCUSSION**

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

879 Organizations review the functions and services provided by systems or system components to
880 determine which functions and services are candidates for elimination. Organizations disable
881 unused or unnecessary physical and logical ports and protocols to prevent the unauthorized
882 connection of devices, the transfer of information, and tunneling. Organizations can utilize
883 network scanning tools, intrusion detection and prevention systems, and end-point protections
884 (e.g., firewalls and host-based intrusion detection systems) to identify and prevent the use of
885 prohibited functions, ports, protocols, and services.

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

891 **REFERENCES**

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

894 **3.4.7.** Withdrawn: Incorporated into 3.4.6.

895 **3.4.8. Authorized Software – Allow by Exception**

- 896 a. Identify software programs authorized to execute on the system.
897 b. Implement a deny-all, allow-by-exception policy to allow the execution of authorized software
898 programs on the system.
899 c. Review and update the list of authorized software programs [*Assignment: organization-*
900 *defined frequency*].

901 **DISCUSSION**

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

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

920 REFERENCES

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

923 3.4.9. User-Installed Software

- 924 a. Establish policies governing the installation of software by users.
925 b. Enforce software installation policies through the following methods: [*Assignment:*
926 *organization-defined methods*].
927 c. Monitor policy compliance [*Assignment: organization-defined frequency*].

928 DISCUSSION

929 Users can install software if provided the necessary privileges. To maintain control over the
930 software installed, organizations identify permitted and prohibited actions regarding software
931 installation. Permitted software installations include updates and security patches to existing
932 software and downloading new applications from organization-approved sources. Prohibited
933 software installations include software with unknown or suspect pedigrees or software that
934 organizations consider potentially malicious. Policies selected for governing user-installed
935 software are organization-developed or provided by some external entity. Policy enforcement
936 methods can include procedural methods and automated methods.

937 REFERENCES

938 Source Controls: [CM-11](#)
939 Supporting Publications: None

940 3.4.10. System Component Inventory

- 941 a. Develop and document an inventory of system components.
942 b. Review and update the system component inventory [*Assignment: organization-defined*
943 *frequency*] and as part of component installations, removals, and system updates.

944 DISCUSSION

945 System components are discrete, identifiable information technology assets that include
946 hardware, software, and firmware. Organizations may choose to implement centralized system
947 component inventories that include components from all organizational systems. In such
948 situations, organizations ensure that the inventories include system-specific information
949 required for component accountability. The information necessary for effective accountability
950 of system components includes the system name, software owners, software version numbers,
951 hardware inventory specifications, software license information, and for networked

952 components, the machine names and network addresses across all implemented protocols (e.g.,
953 IPv4, IPv6). Inventory specifications include the date of receipt, cost, model, serial number,
954 manufacturer, supplier information, component type, and physical location.

955 **REFERENCES**

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

958 **3.4.11. Information Location**

- 959 a. Identify and document the location within the system where CUI is processed and stored.
960 b. Identify and document the users who have access to the system where CUI is processed
961 and stored.
962 c. Document changes to the location where CUI is processed and stored.

963 **DISCUSSION**

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

968 **REFERENCES**

969 Source Controls: [CM-12](#)
970 Supporting Publications: None

971 **3.4.12. System and Component Configuration for High-Risk Areas**

- 972 a. Issue [*Assignment: organization-defined system*] with [*Assignment: organization-defined*
973 *system configurations*] to individuals traveling to locations that the organization deems to be
974 of significant risk.
975 b. Apply the following controls to the system when the individuals return from travel:
976 [*Assignment: organization-defined controls*].

977 **DISCUSSION**

978 When it is known that systems or system components will be in high-risk areas external to the
979 organization, additional controls may be implemented to counter the increased threat. For
980 example, organizations can take actions for notebook computers used by individuals departing
981 on and returning from travel. Actions include determining the locations that are of concern,
982 defining the required configurations for the components, ensuring that components are
983 configured as intended before travel is initiated, and applying controls to the components after
984 travel is completed. Specially configured notebook computers include computers with sanitized
985 hard drives, limited applications, and more stringent configuration settings. Controls applied to
986 mobile devices upon return from travel include examining the mobile device for signs of
987 physical tampering and purging and reimaging disk drives.

988 **REFERENCES**

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

991 **3.5. Identification and Authentication**

992 **3.5.1. User Identification, Authentication, and Re-Authentication**

- 993 a. Uniquely identify and authenticate system user, and associate that unique identification with
994 processes acting on behalf of those users.
- 995 b. Re-authenticate users when [*Assignment: organization-defined circumstances or situations*
996 *requiring re-authentication*].

997 **DISCUSSION**

998 System users include employees or individuals who have equivalent status to employees.
999 Typically, individual identifiers are the usernames associated with the system accounts assigned
1000 to those individuals. Since processes execute on behalf of groups and roles, organizations may
1001 require the unique identification of individuals in group accounts or accountability of individual
1002 activity. The unique identification and authentication of users applies to all system accesses.
1003 Organizations employ passwords, physical authenticators, biometrics or some combination
1004 thereof, to authenticate user identities. Organizations may require the re-authentication of
1005 individuals in certain situations, including when roles, authenticators, or credentials change; when
1006 the execution of privileged functions occurs; after a fixed time period; or periodically.

1007 **REFERENCES**

1008 Source Controls: [IA-2](#), [IA-11](#)
1009 Supporting Publications: SP 800-63-3 [28]

1010 **3.5.2. Device Identification and Authentication**

1011 Uniquely identify and authenticate [*Assignment: organization-defined devices and/or types of*
1012 *devices*] before establishing a system or network connection.

1013 **DISCUSSION**

1014 Devices that require unique device-to-device identification and authentication are defined by
1015 type, device, or a combination of type and device. Organization-defined device types include
1016 devices that are not owned by the organization. Systems use shared known information (e.g.,
1017 Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP]
1018 addresses) for device identification or organizational authentication solutions (e.g., Institute of
1019 Electrical and Electronics Engineers [IEEE] 802.1x and Extensible Authentication Protocol
1020 [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to
1021 identify and authenticate devices on local and wide area networks.

1022 **REFERENCES**

1023 Source Controls: [IA-3](#)
1024 Supporting Publications: SP 800-63-3 [28]

1025 **3.5.3. Multi-Factor Authentication**

1026 Implement multi-factor authentication for access to system accounts.

1027 **DISCUSSION**

1028 Multi-factor authentication requires the use of two or more different factors to achieve
1029 authentication. The authentication factors are defined as follows: something you know (e.g., a
1030 personal identification number [PIN]), something you have (e.g., a physical authenticator, such as
1031 a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication
1032 solutions that feature physical authenticators include hardware authenticators that provide time-
1033 based or challenge-response outputs and smart cards. In addition to authenticating users at the
1034 system level, organizations may also employ authentication mechanisms at the application level
1035 to provide increased information security.

1036 **REFERENCES**

1037 Source Controls: [IA-2\(1\)](#), [IA-2\(2\)](#)
1038 Supporting Publications: SP 800-63-3 [28]

1039 **3.5.4. Replay-Resistant Authentication**

1040 Implement replay-resistant authentication mechanisms for access to system accounts.

1041 **DISCUSSION**

1042 Authentication processes resist replay attacks if it is impractical to successfully authenticate by
1043 recording or replaying previous authentication messages. Replay-resistant techniques include
1044 protocols that use nonces or challenges, such as time synchronous or challenge-response one-time
1045 authenticators.

1046 **REFERENCES**

1047 Source Controls: [IA-2\(8\)](#)
1048 Supporting Publications: SP 800-63-3 [28]

1049 **3.5.5. Identifier Management**

- 1050 a. Receive authorization from [*Assignment: organization-defined personnel or roles*] to assign
1051 an individual, group, role, service, or device identifier.
- 1052 b. Select and assign an identifier that identifies an individual, group, role, service, or device.
- 1053 c. Prevent reuse of identifiers for [*Assignment: organization-defined time period*].
- 1054 d. Identify the status of each individual with the following characteristic: [*Assignment:*
1055 *organization-defined characteristic*].

1056 **DISCUSSION**

1057 Identifiers are provided for users, processes acting on behalf of users, and devices. Preventing the
1058 reuse of identifiers implies preventing the assignment of previously used individual, group, role,
1059 service, or device identifiers to different individuals, groups, roles, services, or devices.
1060 Characteristics that identify the status of individuals include contractors, foreign nationals, and
1061 non-organizational users. Identifying the status of individuals by these characteristics provides
1062 useful information about the people with whom organizational personnel are communicating. For
1063 example, it might be useful for an employee to know that one of the individuals on an email
1064 message is a contractor.

1065 **REFERENCES**

1066 Source Controls: [IA-4](#), [IA-4\(4\)](#)
1067 Supporting Publications: SP 800-63-3 [28]

1068 **3.5.6.** Withdrawn.

1069 **3.5.7. Password Management**

- 1070 a. Enforce the following password composition and complexity rules: [*Assignment: organization-*
1071 *defined composition and complexity rules*].
- 1072 b. Allow user selection of long passwords and passphrases, including spaces and all printable
1073 characters.
- 1074 c. Verify, when users create or update passwords, that the passwords are not found on the list
1075 of commonly-used, expected, or compromised passwords.
- 1076 d. Transmit passwords only over cryptographically-protected channels.
- 1077 e. Store passwords using an approved salted key derivation function, preferably using a keyed
1078 hash.
- 1079 f. Select a new password immediately upon account recovery.
- 1080 g. Allow the use of a temporary password for system logons with an immediate change to a
1081 permanent password.

1082 **DISCUSSION**

1083 Password-based authentication applies to passwords used in single-factor or multi-factor
1084 authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced
1085 composition rules provide marginal security benefits while decreasing usability. However,
1086 organizations may choose to establish certain rules for password generation (e.g., minimum
1087 character length) under certain circumstances and can enforce this requirement. For example,
1088 account recovery can occur when a password is forgotten. Cryptographically protected passwords
1089 include salted one-way cryptographic hashes of passwords. The list of commonly used,
1090 compromised, or expected passwords includes passwords obtained from previous breach
1091 corpus, dictionary words, and repetitive or sequential characters. The list includes context-
1092 specific words, such as the name of the service, username, and derivatives thereof. Changing
1093 temporary passwords to permanent passwords immediately after system logon ensures that the
1094 necessary strength of the authentication mechanism is implemented at the earliest opportunity and
1095 reduces the susceptibility to authenticator compromises.

1096 **REFERENCES**

1097 Source Controls: [IA-5\(1\)](#)
1098 Supporting Publications: SP 800-63-3 [28]

1099 **3.5.8.** Withdrawn.

1100 **3.5.9.** Withdrawn: Incorporated into 3.5.7.

1101 **3.5.10.** Withdrawn: Incorporated into 3.5.7.

1102 **3.5.11. Authentication Feedback**

1103 Obscure feedback of authentication information.

1104 **DISCUSSION**

1105 The feedback from systems does not provide information that would allow unauthorized
1106 individuals to compromise authentication mechanisms. For example, for desktop or notebook
1107 computers with relatively large monitors, the threat may be significant (often referred to as
1108 shoulder surfing). For mobile devices with small displays, this threat may be less significant and
1109 is balanced against the increased likelihood of input errors due to small keyboards. Therefore,
1110 the means for obscuring the authenticator feedback is selected accordingly. Obscuring
1111 authenticator feedback includes displaying asterisks when users type passwords into input
1112 devices or displaying feedback for a limited time before fully obscuring it.

1113 **REFERENCES**

1114 Source Controls: [IA-6](#)
1115 Supporting Publications: None

1116 **3.5.12. Authenticator Management**

- 1117 a. Establish initial authenticator content for any authenticators issued by the organization.
- 1118 b. Verify the identity of the individual, group, role, service, or device receiving the authenticator
1119 as part of the initial authenticator distribution.
- 1120 c. Establish and implement administrative procedures for initial authenticator distribution, for
1121 lost, compromised, or damaged authenticators, and for revoking authenticators.
- 1122 d. Protect authenticator content from unauthorized disclosure and modification.
- 1123 e. Change default authenticators prior to first use.
- 1124 f. Change or refresh authenticators [*Assignment: organization-defined time period by*
1125 *authenticator type*] or when [*Assignment: organization-defined events*].
- 1126 g. Change authenticators for group or role accounts when membership to those accounts
1127 change.

1128 **DISCUSSION**

1129 Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time
1130 password devices, and ID badges. The initial authenticator content is the actual content of the
1131 authenticator (e.g., the initial password). In contrast, requirements for authenticator content
1132 contain specific characteristics. Authenticator management is supported by organization-defined
1133 settings and restrictions for various authenticator characteristics (e.g., password complexity and
1134 composition rules, validation time window for time synchronous one-time tokens, and the
1135 number of allowed rejections during the verification stage of biometric authentication).

1136 The requirement to protect individual authenticators may be implemented by 3.15.3 for
1137 authenticators in the possession of individuals and by 3.1.1, 3.1.2, 3.1.5, and 3.13.8 for
1138 authenticators stored in organizational systems. This includes passwords stored in hashed or
1139 encrypted formats or files that contain encrypted or hashed passwords accessible with
1140 administrator privileges. Actions can be taken to safeguard authenticators, including
1141 maintaining possession of authenticators, not sharing authenticators with others, and
1142 immediately reporting lost, stolen, or compromised authenticators. Developers may deliver
1143 system components with factory default authentication credentials to allow for initial

1144 installation and configuration. Default authentication credentials are often well-known, easily
1145 discoverable, and present a significant risk. Authenticator management includes issuing and
1146 revoking authenticators for temporary access when no longer needed.

1147 **REFERENCES**

1148 Source Controls: [IA-5](#), [IA-5\(6\)](#)
1149 Supporting Publications: None

1150 **3.6. Incident Response**

1151 **3.6.1. Incident Response Plan and Handling**

- 1152 a. Develop an incident response plan that provides the organization with a roadmap for
1153 implementing its incident response capability.
- 1154 b. Implement an incident-handling capability for incidents that is consistent with the incident
1155 response plan and includes preparation, detection and analysis, containment, eradication,
1156 and recovery.
- 1157 c. Update the incident response plan to address system and organizational changes or
1158 problems encountered during plan implementation, execution, or testing.

1159 **DISCUSSION**

1160 It is important that organizations develop and implement a coordinated approach to incident
1161 response. Organizational mission and business functions determine the structure of incident
1162 response capabilities. Incident-related information can be obtained from a variety of sources,
1163 including audit monitoring, network monitoring, physical access monitoring, user and
1164 administrator reports, and reported supply chain events. An effective incident handling capability
1165 involves coordination among many organizational entities, including mission and business
1166 owners, system owners, human resources offices, physical and personnel security offices, legal
1167 departments, operations personnel, and procurement offices.

1168 **REFERENCES**

1169 Source Controls: [IR-4](#), [IR-8](#)
1170 Supporting Publications: SP 800-50 [36], SP 800-61 [51], SP 800-161 [37]

1171 **3.6.2. Incident Monitoring, Reporting, and Response Assistance**

- 1172 a. Track and document system security incidents.
- 1173 b. Report incident information to [*Assignment: organization-defined authorities*].
- 1174 c. Provide an incident response support resource that offers advice and assistance to users of
1175 the system for the handling and reporting of incidents.

1176 **DISCUSSION**

1177 Documenting incidents includes maintaining records about each incident, the status of the
1178 incident, and other pertinent information necessary for forensics as well as evaluating incident
1179 details, trends, and handling. Incident information can be obtained from a variety of sources,
1180 including network monitoring, incident reports, incident response teams, user complaints, supply
1181 chain partners, audit monitoring, physical access monitoring, and user and administrator reports.
1182 3.6.1 provides information on the types of incidents that are appropriate for monitoring. The types

1183 of incidents reported, the content and timeliness of the reports, and the designated reporting
1184 authorities reflect applicable laws, Executive Orders, directives, regulations, policies, standards,
1185 and guidelines. Incident information can inform risk assessments, control effectiveness
1186 assessments, security requirements for acquisitions, and selection criteria for technology
1187 products. Incident response support resources provided by organizations include help desks,
1188 assistance groups, automated ticketing systems to open and track incident response tickets, and
1189 access to forensics services or consumer redress services, when required.

1190 **REFERENCES**

1191 Source Controls: [IR-5](#), [IR-6](#), [IR-7](#)
1192 Supporting Publications: SP 800-61 [51], SP 800-86 [40]

1193 **3.6.3. Incident Response Testing**

1194 Test the effectiveness of the incident response capability [*Assignment: organization-defined*
1195 *frequency*].

1196 **DISCUSSION**

1197 Organizations test incident response capabilities to determine their effectiveness and identify
1198 potential weaknesses or deficiencies. Incident response testing includes the use of checklists,
1199 walk-through or tabletop exercises, and simulations. Incident response testing can include a
1200 determination of the effects of incident response on organizational operations, organizational
1201 assets, and individuals. The use of qualitative and quantitative data aids in determining the
1202 effectiveness of incident response processes.

1203 **REFERENCES**

1204 Source Controls: [IR-3](#)
1205 Supporting Publications: SP 800-84 [52]

1206 **3.6.4. Incident Response Training**

- 1207 a. Provide incident response training to system users consistent with assigned roles and
1208 responsibilities.
- 1209 b. Review and update incident response training content [*Assignment: organization-defined*
1210 *frequency*] and following [*Assignment: organization-defined events*].

1211 **DISCUSSION**

1212 Incident response training is associated with the assigned roles and responsibilities of
1213 organizational personnel to ensure that the appropriate content and level of detail are included in
1214 such training. For example, users may only need to know who to call or how to recognize an
1215 incident; system administrators may require additional training on how to handle incidents; and
1216 incident responders may receive specific training on forensics, data collection techniques,
1217 reporting, system recovery, and system restoration. Incident response training includes user
1218 training in identifying and reporting suspicious activities from external and internal sources.
1219 Incident response training for users may be provided as part of 3.2.2. Events that may precipitate
1220 an update to incident response training content include incident response plan testing, response to
1221 an actual incident, audit or assessment findings, or changes in applicable laws, Executive Orders,
1222 policies, directives, regulations, standards, and guidelines.

1223 **REFERENCES**

1224 Source Controls: [IR-2](#)
1225 Supporting Publications: SP 800-86 [40], SP 800-137 [53]

1226 **3.7. Maintenance**

1227 **3.7.1.** Withdrawn: Recategorized as NCO.

1228 **3.7.2.** Withdrawn: Incorporated into 3.7.4 and 3.7.6.

1229 **3.7.3.** Withdrawn: Incorporated into 3.8.3.

1230 **3.7.4. Maintenance Tools**

- 1231 a. Approve, control, and monitor the use of system maintenance tools.
- 1232 b. Inspect maintenance tools and media containing diagnostic and test programs for malicious
1233 code before the media and tools are used in the system.
- 1234 c. Prevent the removal of maintenance equipment containing CUI by:
- 1235 1. Verifying that there is no CUI on the equipment;
- 1236 2. Sanitizing or destroying the equipment; or
- 1237 3. Obtaining an exemption from [*Assignment: organization-defined officials*] explicitly
1238 authorizing removal of the equipment from the facility.

1239 **DISCUSSION**

1240 Approving, controlling, monitoring, and reviewing maintenance tools address security-related
1241 issues associated with the tools that are used for diagnostic and repair actions on the system.
1242 Maintenance tools can include hardware and software diagnostic and test equipment as well as
1243 packet sniffers. The tools may be pre-installed, brought in with maintenance personnel on media,
1244 cloud-based, or downloaded from a website. Diagnostic and test programs are potential vehicles
1245 for transporting malicious code into the system, either intentionally or unintentionally. Examples
1246 of media inspection include checking the cryptographic hash or digital signatures of diagnostic
1247 and test programs and/or media. If, upon inspection of media that contain maintenance diagnostic
1248 and test programs, organizations determine that the media contain malicious code, the incident is
1249 handled consistent with incident handling policies and procedures. A periodic review of system
1250 maintenance tools can result in the withdrawal of approval for outdated, unsupported, irrelevant,
1251 or no-longer-used tools. The hardware and software components that support maintenance and
1252 are considered a part of the system (including software implementing utilities such as “ping,”
1253 “ls,” “ipconfig,” or hardware and software that implement the monitoring port of an Ethernet
1254 switch) are not addressed by maintenance tools.

1255 **REFERENCES**

1256 Source Controls: [MA-3](#), [MA-3\(1\)](#), [MA-3\(2\)](#), [MA-3\(3\)](#)
1257 Supporting Publications: SP 800-88 [54]

1258 **3.7.5. Nonlocal Maintenance**

- 1259 a. Approve and monitor nonlocal maintenance and diagnostic activities.
- 1260 b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal
- 1261 maintenance and diagnostic sessions.
- 1262 c. Terminate session and network connections when nonlocal maintenance is completed.

1263 **DISCUSSION**

1264 Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate

1265 through either an external or internal network. Local maintenance and diagnostic activities are

1266 carried out by individuals who are physically present at the system location and not

1267 communicating across a network connection. Authentication techniques used to establish

1268 nonlocal maintenance and diagnostic sessions reflect the requirements in 3.5.1.

1269 **REFERENCES**

1270 Source Controls: [MA-4](#)

1271 Supporting Publications: SP 800-63-3 [28], SP 800-88 [54]

1272 **3.7.6. Maintenance Personnel**

- 1273 a. Establish a process for maintenance personnel authorization, and maintain a list of
- 1274 authorized maintenance organizations or personnel.
- 1275 b. Verify that non-escorted personnel who perform maintenance on the system possess the
- 1276 required access authorizations.
- 1277 c. Designate organizational personnel with required access authorizations and technical
- 1278 competence to supervise the maintenance activities of personnel who do not possess the
- 1279 required access authorizations.

1280 **DISCUSSION**

1281 Maintenance personnel refers to individuals who perform hardware or software maintenance on

1282 the system, while 3.10.1 addresses physical access for individuals whose maintenance duties

1283 place them within the physical protection perimeter of the system. Technical competence of

1284 supervising individuals relates to the maintenance performed on the system, while having

1285 required access authorizations refers to maintenance on and near the system. Individuals not

1286 previously identified as authorized maintenance personnel (e.g., manufacturers, consultants,

1287 systems integrators, and vendors) may require privileged access to the system, such as when they

1288 are required to conduct maintenance with little or no notice. Organizations may choose to issue

1289 temporary credentials to these individuals based on their risk assessments. Temporary credentials

1290 may be for one-time use or for very limited time periods.

1291 **REFERENCES**

1292 Source Controls: [MA-5](#)

1293 Supporting Publications: None

1294 **3.8. Media Protection**

1295 **3.8.1. Media Storage**

1296 Physically control and securely store digital and non-digital media containing CUI until the media
1297 are destroyed or sanitized using approved equipment, techniques, and procedures.

1298 **DISCUSSION**

1299 Digital media includes diskettes, flash drives, magnetic tapes, external or removable solid state or
1300 magnetic drives, compact discs, and digital versatile discs. Non-digital media includes paper and
1301 microfilm. Physically controlling stored media includes conducting inventories, establishing
1302 procedures to allow individuals to check out and return media to libraries, and maintaining
1303 accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a
1304 controlled media library. Controlled areas provide physical and procedural controls to meet the
1305 requirements established for protecting information and systems.

1306 **REFERENCES**

1307 Source Controls: [MP-4](#)
1308 Supporting Publications: SP 800-111 [55]

1309 **3.8.2. Media Access**

1310 Restrict access to CUI on digital and non-digital media to [*Assignment: organization-defined*
1311 *personnel or roles*].

1312 **DISCUSSION**

1313 Access to CUI on system media can be restricted by physically controlling such media, which
1314 includes conducting inventories, ensuring that procedures are in place to allow individuals to
1315 check out and return media to the media library, and maintaining accountability for stored media.

1316 **REFERENCES**

1317 Source Controls: [MP-2](#)
1318 Supporting Publications: SP 800-111 [55]

1319 **3.8.3. Media Sanitization**

1320 Sanitize system media containing CUI prior to maintenance, disposal, release out of
1321 organizational control, or release for reuse.

1322 **DISCUSSION**

1323 Media sanitization applies to all digital and non-digital system media subject to disposal or reuse,
1324 whether or not the media is considered removable. Examples include digital media in scanners,
1325 copiers, printers, notebook computers, workstations, mobile devices, network components, and
1326 non-digital media. The sanitization process removes CUI from system media such that the
1327 information cannot be retrieved or reconstructed. Sanitization techniques (e.g., clearing, purging,
1328 cryptographically erasing, and destroying) prevent the disclosure of information to unauthorized
1329 individuals when such media is reused or released for disposal. Organizations determine the
1330 appropriate sanitization methods with the recognition that destruction is sometimes necessary

1331 when other methods cannot be applied to media that require sanitization. NARA policies control
1332 the sanitization process for CUI.

1333 **REFERENCES**

1334 Source Controls: [MP-6](#)
1335 Supporting Publications: SP 800-88 [54]

1336 **3.8.4. Media Marking**

- 1337 a. Mark system media containing CUI indicating distribution limitations, handling caveats, and
1338 security markings.
- 1339 b. Exempt [*Assignment: organization-defined types of system media containing CUI*] from
1340 marking if the media remain within [*Assignment: organization-defined controlled areas*].

1341 **DISCUSSION**

1342 Security marking refers to the application or use of human-readable security attributes. Security
1343 labeling refers to the use of security attributes for internal system data structures. Digital media
1344 includes diskettes, magnetic tapes, external or removable solid state or magnetic drives, flash
1345 drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm.
1346 CUI is defined by NARA along with appropriate safeguarding and dissemination requirements
1347 for such information.

1348 **REFERENCES**

1349 Source Controls: [MP-3](#)
1350 Supporting Publications: None

1351 **3.8.5. Media Transport**

- 1352 a. Protect, control, and maintain accountability for system media containing CUI and during
1353 transport outside of controlled areas.
- 1354 b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI stored
1355 on digital media during transport.

1356 **DISCUSSION**

1357 System media includes digital and non-digital media. Digital media includes flash drives,
1358 diskettes, magnetic tapes, external or removable solid state or magnetic drives, compact discs,
1359 and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are
1360 spaces for which organizations provide physical or procedural controls to meet the requirements
1361 established for protecting information and systems. Controls to protect media during transport
1362 include cryptography and locked containers. Cryptographic mechanisms can provide
1363 confidentiality protections, depending on the mechanisms implemented. Activities associated
1364 with media transport include releasing media for transport, ensuring that media enters the
1365 appropriate transport processes, and the actual transport. Authorized transport and courier
1366 personnel may include individuals external to the organization. Maintaining accountability of
1367 system media during transport includes restricting transport activities to authorized personnel and
1368 tracking or obtaining records of transport activities as the media moves through the transportation
1369 system to prevent and detect loss, destruction, or tampering.

1370 **REFERENCES**

1371 Source Controls: [MP-5](#), [SC-28](#), [SC-28\(1\)](#)
1372 Supporting Publications: SP 800-111 [55]

1373 **3.8.6.** Withdrawn: Incorporated into 3.8.5.

1374 **3.8.7. Media Use**

1375 a. [*Selection: Restrict; Prohibit*] the use of [*Assignment: organization-defined removable system*
1376 *media*].

1377 b. Prohibit the use of portable storage devices when such devices have no identifiable owner.

1378 **DISCUSSION**

1379 In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts
1380 the use of certain types of media on systems, such as restricting or prohibiting the use of flash
1381 drives or external hard drives. Organizations can employ technical and nontechnical controls
1382 (e.g., policies, procedures, and rules of behavior) to control the use of system media. For
1383 example, organizations may control the use of portable storage devices by using physical cages
1384 on workstations to prohibit access to external ports or disabling or removing the ability to insert,
1385 read, or write to devices.

1386 Organizations may limit the use of portable storage devices to only approved devices, including
1387 devices provided by the organization, devices provided by other approved organizations, and
1388 devices that are not personally owned. Finally, organizations may control the use of portable
1389 storage devices based on the type of device – prohibiting the use of writeable, portable devices –
1390 and implement this restriction by disabling or removing the capability to write to such devices.
1391 Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage
1392 devices reduces the risk of using such technologies by allowing organizations to assign
1393 responsibility and accountability for addressing known vulnerabilities in the devices (e.g.,
1394 insertion of malicious code).

1395 **REFERENCES**

1396 Source Controls: [MP-7](#)
1397 Supporting Publications: SP 800-111 [55]

1398 **3.8.8.** Withdrawn: Incorporated into 3.8.7.

1399 **3.8.9. System Backup – Cryptographic Protection**

1400 Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup
1401 storage locations.

1402 **DISCUSSION**

1403 Organizations can employ cryptographic mechanisms or alternative physical controls to protect
1404 the confidentiality of backup information at designated storage locations. Backed-up information
1405 that contains CUI may include system-level information and user-level information. System-level
1406 information includes system-state information, operating system software, application software,
1407 and licenses. User-level information includes information other than system-level information.

1408 **REFERENCES**

1409 Source Controls: [CP-9\(8\)](#)
1410 Supporting Publications: SP 800-34 [56], SP 800-130 [57], SP 800-152 [58]

1411 **3.9. Personnel Security**

1412 **3.9.1. Personnel Screening**

- 1413 a. Screen individuals prior to authorizing access to the system.
1414 b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions*
1415 *requiring rescreening*].

1416 **DISCUSSION**

1417 Personnel security screening activities involve the assessment of an individual's conduct,
1418 integrity, judgment, loyalty, reliability, and stability (i.e., the individual's trustworthiness) prior to
1419 authorizing access to the system. The screening activities reflect applicable federal laws,
1420 Executive Orders, directives, policies, regulations, and criteria established for the level of access
1421 required for the assigned position.

1422 **REFERENCES**

1423 Source Controls: [PS-3](#)
1424 Supporting Publications: SP 800-181 [38]

1425 **3.9.2. Personnel Termination and Transfer**

- 1426 a. When individual employment is terminated:
1427 1. Disable system access within [*Assignment: organization-defined time period*];
1428 2. Terminate or revoke authenticators and credentials associated with the individual; and
1429 3. Retrieve all security-related system property.
1430 b. When individuals are reassigned or transferred to other positions within the organization:
1431 1. Review and confirm the ongoing operational need for current logical and physical access
1432 authorizations to the system and facility;
1433 2. Initiate [*Assignment: organization-defined transfer or reassignment actions*] within
1434 [*Assignment: organization-defined time period following the formal transfer action*]; and
1435 3. Modify access authorization as needed to correspond with any changes in operational
1436 need due to reassignment or transfer.

1437 **DISCUSSION**

1438 Security-related system property includes hardware authentication tokens, system administration
1439 technical manuals, keys, identification cards, and building passes. Exit interviews ensure that
1440 terminated individuals understand the security constraints imposed by being former employees
1441 and that accountability is achieved for the organizational property. Security topics at exit
1442 interviews include reminding individuals of potential limitations on future employment and
1443 nondisclosure agreements. Exit interviews may not always be possible for some individuals,
1444 including in cases related to the unavailability of supervisors, illnesses, or job abandonment.

1445 The timely execution of termination actions is essential for individuals who have been terminated
1446 for cause. Organizations may consider disabling the accounts of individuals who are being
1447 terminated prior to the individuals being notified. This requirement applies to the reassignment or
1448 transfer of individuals when the personnel action is permanent or of such extended duration as to
1449 require protection. Protections that may be required for transfers or reassignments to other
1450 positions within organizations include returning old and issuing new identification cards, keys,
1451 and building passes; changing system access authorizations (i.e., privileges); closing system
1452 accounts and establishing new accounts; and providing access to official records to which
1453 individuals had access at previous work locations in previous system accounts.

1454 **REFERENCES**

1455 Source Controls: [PS-4](#), [PS-5](#)
1456 Supporting Publications: None

1457 **3.9.3. External Personnel Security**

- 1458 a. Establish and document personnel security requirements, including security roles and
1459 responsibilities for external providers.
- 1460 b. Require external providers to comply with the personnel security policies and procedures
1461 established by the organization.
- 1462 c. Monitor provider compliance with personnel security requirements.

1463 **DISCUSSION**

1464 External providers include contractors and other organizations that provide system development,
1465 information technology services, testing or assessment services, outsourced applications, cloud
1466 services, and network or security management. Organizations explicitly include personnel
1467 security requirements in acquisition-related documents. External providers may have personnel
1468 who work at organizational facilities with credentials, badges, or system privileges issued by
1469 organizations.

1470 **REFERENCES**

1471 Source Controls: [PS-7](#)
1472 Supporting Publications: None

1473 **3.10. Physical Protection**

1474 **3.10.1. Physical Access Authorizations**

- 1475 a. Develop, approve, and maintain a list of individuals with authorized access to the facility
1476 where the system resides.
- 1477 b. Issue authorization credentials for facility access.
- 1478 c. Review the access list detailing authorized facility access by individuals [*Assignment:*
1479 *organization-defined frequency*].
- 1480 d. Remove individuals from the facility access list when access is no longer required.

1481

DISCUSSION

1482 Physical access authorizations apply to employees and visitors. Individuals with permanent
1483 physical access authorization credentials are not considered visitors. Authorization credentials
1484 include ID badges, identification cards, and smart cards. Organizations determine the strength
1485 of authorization credentials needed consistent with applicable laws, Executive Orders,
1486 directives, regulations, policies, standards, and guidelines. Physical access authorizations may
1487 not be necessary to access certain areas within facilities that are designated as publicly
1488 accessible.

1489

REFERENCES

1490

Source Controls: [PE-2](#)

1491

Supporting Publications: None

1492 3.10.2. Monitoring Physical Access

- 1493 a. Monitor physical access to the facility where the system resides to detect and respond to
1494 physical security incidents.
- 1495 b. Review physical access logs [*Assignment: organization-defined frequency*] and upon
1496 occurrence of [*Assignment: organization-defined events or potential indications of events*].
- 1497 c. Coordinate the results of reviews and investigations with the organizational incident
1498 response capability.

1499

DISCUSSION

1500 Physical access monitoring includes publicly accessible areas within organizational facilities.
1501 Examples of physical access monitoring include the employment of guards, video surveillance
1502 equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify
1503 suspicious activity, anomalous events, or potential threats. The reviews can be supported by
1504 audit logging controls if the access logs are part of an automated system. Organizational
1505 incident response capabilities include investigations of physical security incidents and responses
1506 to the incidents. Incidents include security violations or suspicious physical access activities,
1507 such as access outside of normal work hours, repeated access to areas not normally accessed,
1508 access for unusual lengths of time, and out-of-sequence access.

1509

REFERENCES

1510

Source Controls: [PE-6](#)

1511

Supporting Publications: None

1512 **3.10.3.** Withdrawn: Incorporated into 3.10.7.

1513 **3.10.4.** Withdrawn: Incorporated into 3.10.7.

1514 **3.10.5.** Withdrawn: Incorporated into 3.10.7.

1515 3.10.6. Alternate Work Site

- 1516 a. Determine and document alternate work sites allowed for use by employees.

- 1517 b. Employ the following controls at alternate work sites: [*Assignment: organization-defined*
1518 *controls*].

1519 **DISCUSSION**

1520 Alternate work sites include the private residences of employees or other facilities designated
1521 by the organization. Alternate work sites can provide readily available alternate locations during
1522 contingency operations. Organizations can define different sets of controls for specific alternate
1523 work sites or types of sites depending on the work-related activities conducted at the sites.
1524 Implementing and assessing the effectiveness of organization-defined controls and providing a
1525 means to communicate incidents at alternate work sites supports the contingency planning
1526 activities of organizations.

1527 **REFERENCES**

1528 Source Controls: [PE-17](#)
1529 Supporting Publications: SP 800-46 [15], SP 800-114 [21]

1530 **3.10.7. Physical Access Control**

- 1531 a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit*
1532 *points to the facility where the system resides*] by:
- 1533 1. Verifying individual access authorizations before granting access to the facility; and
 - 1534 2. Controlling ingress and egress to the facility using [*Selection (one or more):*
1535 *[Assignment: organization-defined physical access control systems or devices];*
1536 *guards*].
- 1537 b. Maintain physical access audit logs for [*Assignment: organization-defined entry or exit*
1538 *points*].
- 1539 c. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances*
1540 *requiring visitor escorts and control of visitor activity*].
- 1541 d. Secure keys, combinations, and other physical access devices.

1542 **DISCUSSION**

1543 Physical access control applies to employees and visitors. Individuals with permanent physical
1544 access authorizations are not considered visitors. Organizations determine the types of guards
1545 needed, including professional security staff or administrative staff. Physical access devices
1546 include keys, locks, combinations, biometric readers, and card readers. Physical access control
1547 systems comply with applicable laws, Executive Orders, directives, policies, regulations,
1548 standards, and guidelines. Organizations have flexibility in the types of audit logs employed.
1549 Audit logs can be procedural, automated, or some combination thereof. Physical access points
1550 can include facility access points, interior access points to systems that require supplemental
1551 access controls, or both.

1552 **REFERENCES**

1553 Source Controls: [PE-3](#)
1554 Supporting Publications: None

1555 3.10.8. Access Control for Transmission and Output Devices

- 1556 a. Control physical access to system distribution and transmission lines within organizational
1557 facilities.
- 1558 b. Control physical access to output from [*Assignment: organization-defined output devices*] to
1559 prevent unauthorized individuals from obtaining the output.

1560 DISCUSSION

1561 Safeguarding measures applied to system distribution and transmission lines prevent accidental
1562 damage, disruption, and physical tampering. Such controls may also be necessary to prevent
1563 eavesdropping or the modification of unencrypted transmissions. Security controls used to
1564 control physical access to system distribution and transmission lines include disconnected or
1565 locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and
1566 wiretapping sensors. Controlling physical access to output devices includes placing output
1567 devices in locked rooms or other secured areas with keypad or card reader access controls and
1568 allowing access to authorized individuals only, placing output devices in locations that can be
1569 monitored by personnel, installing monitor or screen filters, and using headphones. Examples of
1570 output devices include monitors, printers, scanners, audio devices, facsimile machines, and
1571 copiers.

1572 REFERENCES

1573 Source Controls: [PE-4](#), [PE-5](#)
1574 Supporting Publications: None

1575 3.11. Risk Assessment

1576 3.11.1. Risk Assessment

- 1577 a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the
1578 processing, storage, or transmission of CUI.
- 1579 b. Update risk assessments (including supply chain risk) [*Assignment: organization-defined*
1580 *frequency*].

1581 DISCUSSION

1582 Clearly defined system boundaries are a prerequisite for effective risk assessments. Risk
1583 assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations
1584 and assets based on the operation and use of the system. Risk assessments also consider risk
1585 from external parties (e.g., service providers, contractors operating systems on behalf of the
1586 organization, individuals accessing systems, outsourcing entities). Risk assessments, either
1587 formal or informal, can be conducted at the organization level, the mission or business process
1588 level, or the system level and at any phase in the system development life cycle.

1589 Risk assessments include supply chain-related risks associated with suppliers or contractors and
1590 the system, system component, or system service that they provide. Supply chain events that
1591 affect risk include disruption, the use of defective components, the insertion of counterfeits,
1592 theft, malicious development practices, improper delivery practices, and the insertion of
1593 malicious code. These events can have a significant impact on the system and its information
1594 and, therefore, can also adversely impact organizations. The supply chain events may be
1595 unintentional or malicious and can occur at any point in the system life cycle.

1596 **REFERENCES**

1597 Source Controls: [RA-3](#), [RA-3\(1\)](#), [SR-6](#)
1598 Supporting Publications: SP 800-30 [59], SP 800-161 [37]

1599 **3.11.2. Vulnerability Monitoring and Scanning**

- 1600 a. Monitor and scan for vulnerabilities in the system [*Assignment: organization-defined*
1601 *frequency*] and when new vulnerabilities affecting the system are identified.
- 1602 b. Remediate vulnerabilities [*Assignment: organization-defined response times*] in accordance
1603 with an organizational assessment of risk.
- 1604 c. Update vulnerabilities to be scanned [*Assignment: organization-defined frequency*].
- 1605 d. Implement privileged access authorization to the system for vulnerability scanning activities.

1606 **DISCUSSION**

1607 Organizations determine the required vulnerability scanning for system components (including
1608 hardware, software, firmware, and applications) and ensure that potential sources of
1609 vulnerabilities (e.g., networked printers, scanners, and copiers) are not overlooked. The
1610 vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered and
1611 announced and new scanning methods are developed. This process ensures that potential
1612 vulnerabilities in the system are identified and addressed as quickly as possible.

1613 Vulnerability analyses for custom software may require additional approaches, such as static
1614 analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations
1615 can employ these analysis approaches in source code reviews and in a variety of tools (e.g.,
1616 static analysis tools, web-based application scanners, binary analyzers). Vulnerability scanning
1617 includes scanning for patch levels; scanning for functions, ports, protocols, and services that
1618 should not be accessible to users or devices; and scanning for improperly configured or
1619 incorrectly operating information flow control mechanisms.

1620 To facilitate interoperability, organizations consider using products that are Security Content
1621 Automated Protocol (SCAP)-validated, as well as scanning tools that express vulnerabilities in
1622 the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the
1623 Open Vulnerability Assessment Language (OVAL) to determine the presence of system
1624 vulnerabilities. Sources for vulnerability information include the Common Weakness
1625 Enumeration (CWE) listing and the National Vulnerability Database (NVD).

1626 Security assessments, such as red team exercises, provide additional sources of potential
1627 vulnerabilities for which to scan. Organizations also consider using scanning tools that express
1628 vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain
1629 situations, the nature of the vulnerability scanning may be more intrusive, or the system
1630 component that is the subject of the scanning may contain highly sensitive information.
1631 Privileged access authorization to selected system components facilitates thorough vulnerability
1632 scanning and protects the sensitive nature of such scanning.

1633 **REFERENCES**

1634 Source Controls: [RA-5](#), [RA-5\(2\)](#), [RA-5\(5\)](#)
1635 Supporting Publications: SP 800-40 [60], SP 800-53A [61], SP 800-70 [48], SP 800-115 [62],
1636 SP 800-126 [49]

1637 **3.11.3. Withdrawn: Incorporated into 3.11.2.**

1638 **3.11.4. Risk Response**

1639 Respond to findings from security assessments, monitoring, and audits.

1640 **DISCUSSION**

1641 Organizations have many options for responding to risk, including mitigating risk by
1642 implementing new controls or strengthening existing controls, accepting risk with appropriate
1643 justification or rationale, sharing or transferring risk, or avoiding risk. The organizational risk
1644 management strategy and risk tolerance influence risk response decisions and actions. This
1645 requirement addresses the need to determine an appropriate response to risk before generating a
1646 plan of action and milestones entry. For example, the response may be to accept risk or reject
1647 risk, or it may be possible to mitigate the risk immediately so that a plan of action and
1648 milestones entry is not needed. However, if the risk response is to mitigate the risk, and the
1649 mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

1650 **REFERENCES**

1651 Source Controls: [RA-7](#)

1652 Supporting Publications: SP 800-30 [59], SP 800-37 [63], SP 800-39 [64], SP 800-160-1 [12]

1653 **3.12. Security Assessment and Monitoring**

1654 **3.12.1. Control Assessments**

1655 Assess the controls in the system and its environment of operation [*Assignment: organization-*
1656 *defined frequency*] to determine the extent to which the controls are implemented correctly,
1657 operating as intended, and producing the desired outcome with respect to meeting specified
1658 security requirements.

1659 **DISCUSSION**

1660 Organizations assess security controls in the system and the environment in which that system
1661 operates as part of the system development life cycle. Security controls are the safeguards that
1662 organizations implement to satisfy security requirements. By assessing implemented security
1663 controls, organizations determine whether the necessary safeguards are in place and operating
1664 as intended. Security control assessments identify weaknesses and deficiencies early in the
1665 system life cycle, provide essential information needed to make risk-based decisions, and ensure
1666 compliance to vulnerability mitigation procedures. Assessments are conducted on the
1667 implemented controls as documented in system security plans.

1668 Security assessment reports document assessment results in sufficient detail as deemed
1669 necessary by organizations to determine the accuracy and completeness of the reports and
1670 whether the security controls are implemented correctly, operating as intended, and producing
1671 the desired outcome with respect to meeting security requirements. Security assessment results
1672 are provided to the individuals or roles appropriate for the types of assessments being
1673 conducted.

1674 Organizations ensure that assessment results are current, relevant to the determination of control
1675 effectiveness, and obtained with the appropriate level of assessor independence. Organizations
1676 can choose to use other types of assessment activities, such as vulnerability scanning and
1677 system monitoring, to maintain the security posture of the system during the system life cycle.

1678 **REFERENCES**

1679 Source Controls: [CA-2](#)
1680 Supporting Publications: SP 800-53 [8], SP 800-53A [61], SP 800-37 [63], SP 800-115 [62]

1681 **3.12.2. Plan of Action and Milestones**

- 1682 a. Develop a plan of action and milestones for the system:
- 1683 1. To document the planned remediation actions to correct weaknesses or deficiencies
1684 noted during control assessments; and
 - 1685 2. To reduce or eliminate known vulnerabilities in the system.
- 1686 b. Update the existing plan of action and milestones [*Assignment: organization-defined*
1687 *frequency*] based on the findings from control assessments, independent audits or reviews,
1688 and continuous monitoring activities.

1689 **DISCUSSION**

1690 Plans of action and milestones (POAMs) are important documents in organizational security
1691 programs. Organizations use POAMs to describe how unimplemented security requirements
1692 and security controls will be met and how planned mitigations will be implemented.
1693 Organizations can document system security plans and POAMs as separate or combined
1694 documents and in any chosen format. Federal agencies may consider system security plans and
1695 POAMs as inputs to risk-based decisions on whether to process, store, or transmit CUI on a
1696 system hosted by a nonfederal organization.

1697 **REFERENCES**

1698 Source Controls: [CA-5](#)
1699 Supporting Publications: SP 800-37 [63]

1700 **3.12.3. Continuous Monitoring**

1701 Develop and implement a system-level continuous monitoring strategy that includes ongoing
1702 monitoring and assessment of control effectiveness.

1703 **DISCUSSION**

1704 Continuous monitoring at the system level facilitates ongoing awareness of the system security
1705 posture to support organizational risk management decisions. The terms *continuous* and
1706 *ongoing* imply that organizations assess and monitor their controls and risks at a frequency
1707 sufficient to support risk-based decisions. Different types of controls may require different
1708 monitoring frequencies. When monitoring the effectiveness of multiple controls that have been
1709 grouped into capabilities, a root cause analysis may be needed to determine the specific control
1710 that has failed.

1711 **REFERENCES**

1712 Source Controls: [CA-7](#)
1713 Supporting Publications: SP 800-37 [63], SP 800-39 [64], SP 800-53A [61], SP 800-115 [62],
1714 SP 800-137 [53]

1715 **3.12.4. Withdrawn: Incorporated into 3.15.2.**

1716 **3.12.5. Independent Assessment**

1717 Use independent assessors or assessment teams to assess controls.

1718 **DISCUSSION**

1719 Independent assessors or assessment teams are individuals or groups who conduct impartial
1720 security assessments of the system. Impartiality means that assessors are free from perceived or
1721 actual conflicts of interest regarding the development, operation, sustainment, or management
1722 of the system under assessment or the determination of control effectiveness. To achieve
1723 impartiality, assessors do not create a mutual or conflicting interest with the organizations
1724 where the assessments are being conducted, assess their own work, act as management or
1725 employees of the organizations they are serving, or place themselves in positions of advocacy
1726 for the organizations that acquire their services.

1727 **REFERENCES**

1728 Source Controls: [CA-2\(1\)](#)

1729 Supporting Publications: SP 800-37 [63], SP 800-53A [61], SP 800-115 [62], SP 800-137 [53]

1730 **3.12.6. Information Exchange**

1731 a. Approve, document, and manage the exchange of CUI between the system and other
1732 systems using [*Assignment: organization-defined agreements*].

1733 b. Review and update the agreements [*Assignment: organization-defined frequency*].

1734 **DISCUSSION**

1735 The types of agreements selected are based on factors such as the relationship between the
1736 organizations exchanging information (e.g., government to government, government to
1737 business, business to business, government or business to service provider, government or
1738 business to individual) or the level of access to the organizational system by users of the other
1739 system. Types of agreements can include interconnection security agreements, information
1740 exchange security agreements, memoranda of understanding or agreement, service-level
1741 agreements, or other types of agreements. Organizations may incorporate agreement
1742 information into formal contracts, especially for information exchanges established between
1743 federal agencies and nonfederal organizations (e.g., service providers, contractors, system
1744 developers, and system integrators). Examples of the types of information contained in
1745 exchange agreements include the interface characteristics, security requirements, controls, and
1746 responsibilities for each system.

1747 **REFERENCES**

1748 Source Controls: [CA-3](#)

1749 Supporting Publications: SP 800-47 [87]

1750 **3.12.7. Internal System Connections**

1751 a. Authorize internal system connections of [*Assignment: organization-defined system*
1752 *components or classes of components*].

1753 b. Review the continued need for each internal system connection [*Assignment: organization-*
1754 *defined frequency*].

1755 **DISCUSSION**

1756 Internal system connections are connections between the organizational system and separate
1757 constituent system components (i.e., connections between components that are part of the same
1758 system), including components used for system development. Intra-system connections include
1759 connections with mobile devices, notebook and desktop computers, tablets, printers, copiers,
1760 facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system
1761 connection, organizations can authorize internal connections for a class of system components
1762 with common characteristics and/or configurations, including printers, scanners, and copiers
1763 with a specified processing, transmission, and storage capability or smart phones and tablets
1764 with a specific baseline configuration.

1765 **REFERENCES**

1766 Source Controls: [CA-9](#)
1767 Supporting Publications: SP 800-124 [29]

1768 **3.13. System and Communications Protection**

1769 **3.13.1. Boundary Protection**

- 1770 a. Monitor and control communications at the external managed interfaces to the system and
1771 at key internal managed interfaces within the system.
- 1772 b. Implement subnetworks for publicly accessible system components that are physically or
1773 logically separated from internal networks.
- 1774 c. Connect to external networks or systems only through managed interfaces consisting of
1775 boundary protection devices arranged in accordance with an organizational security
1776 architecture.

1777 **DISCUSSION**

1778 Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code
1779 analysis, virtualization systems, or encrypted tunnels implemented within a security
1780 architecture. Subnetworks that are either physically or logically separated from internal
1781 networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces
1782 within organizational systems includes restricting external web traffic to designated web servers
1783 within managed interfaces, prohibiting external traffic that appears to be spoofing internal
1784 addresses, and prohibiting internal traffic that appears to be spoofing external addresses.
1785 Boundary protection may be implemented as a common control for all or part of an
1786 organizational network such that the boundary to be protected is greater than a system-specific
1787 boundary (i.e., an authorization boundary).

1788 Organizations consider the shared nature of commercial telecommunications services in the
1789 implementation of security requirements associated with the use of such services. Commercial
1790 telecommunications services are commonly based on network components and consolidated
1791 management systems shared by all attached commercial customers and may also include third
1792 party-provided access lines and other service elements. Such transmission services may
1793 represent sources of increased risk despite contract security provisions.

1794 **REFERENCES**

1795 Source Controls: [SC-7](#)

1796 Supporting Publications: SP 800-41 [68], SP 800-125B [69], SP 800-160-1 [12], SP 800-189
1797 [71], SP 800-207 [70]

1798 **3.13.2.** Withdrawn: Incorporated into 3.16.1.

1799 **3.13.3. Separation of System and User Functionality**

1800 Separate user functionality from system management functionality.

1801 **DISCUSSION**

1802 System management functionality includes the functions necessary to administer databases,
1803 network components, workstations, or servers and typically requires privileged user access. The
1804 separation of user functionality from system management functionality is physical or logical.
1805 Organizations can implement the separation of system management functionality from user
1806 functionality by using different computers, different central processing units, different instances
1807 of operating systems, different network addresses, virtualization techniques, or combinations of
1808 these or other methods, as appropriate. This type of separation includes web administrative
1809 interfaces that use separate authentication methods for users of any other system resources. The
1810 separation of functionality may include isolating administrative interfaces on different domains
1811 and with additional access controls.

1812 **REFERENCES**

1813 Source Controls: [SC-2](#)
1814 Supporting Publications: SP 800-160-1 [12]

1815 **3.13.4. Information in Shared System Resources**

1816 Prevent unauthorized and unintended information transfer via shared system resources.

1817 **DISCUSSION**

1818 Preventing unauthorized and unintended information transfer via shared system resources stops
1819 information produced by the actions of prior users or roles (or actions of processes acting on
1820 behalf of prior users or roles) from being available to current users or roles (or current processes
1821 acting on behalf of current users or roles) that obtain access to shared system resources after
1822 those resources have been released back to the system. Information in shared system resources
1823 also applies to encrypted representations of information. In other contexts, the control of
1824 information in shared system resources is referred to as object reuse and residual information
1825 protection. Information in shared system resources does not address information remanence,
1826 which refers to the residual representation of data that has been nominally deleted, covert
1827 channels (including storage and timing channels) in which shared system resources are
1828 manipulated to violate information flow restrictions, or components within systems for which
1829 there are only single users or roles.

1830 **REFERENCES**

1831 Source Controls: [SC-4](#)
1832 Supporting Publications: None

1833 **3.13.5.** Withdrawn: Incorporated into 3.13.1.

1834 **3.13.6. Network Communications – Deny by Default – Allow by Exception**

1835 Deny network communications traffic by default, and allow network communications traffic by
1836 exception.

1837 **DISCUSSION**

1838 This requirement applies to inbound and outbound network communications traffic at the
1839 system boundary and at identified points within the system. A deny-all, allow-by-exception
1840 network communications traffic policy ensures that only essential and approved connections are
1841 allowed.

1842 **REFERENCES**

1843 Source Controls: [SC-7\(5\)](#)
1844 Supporting Publications: SP 800-41 [68], SP 800-77 [19], SP 800-189 [71]

1845 **3.13.7. Split Tunneling**

1846 Prevent split tunneling for remote devices unless the split tunnel is securely provisioned using
1847 [*Assignment: organization-defined safeguards*].

1848 **DISCUSSION**

1849 Split tunneling is the process of allowing a remote user or device to establish a non-remote
1850 connection with a system and simultaneously communicate with a resource in an external
1851 network via some other connection. This method of network access enables a user to access
1852 remote devices and simultaneously access uncontrolled networks. Split tunneling may be
1853 desirable by remote users to communicate with system resources, such as printers or file
1854 servers. However, split tunneling can facilitate unauthorized external connections and make the
1855 system vulnerable to attack and the exfiltration of CUI.

1856 Split tunneling can be prevented by disabling configuration settings that allow such capabilities
1857 in remote devices and by preventing those configuration settings from being configurable by
1858 users. Prevention can also be achieved through the detection of split tunneling (or of
1859 configuration settings that allow split tunneling) in the remote device and by prohibiting the
1860 connection if the remote device is using split tunneling. A virtual private network (VPN) can be
1861 used to securely provision a split tunnel. A securely provisioned VPN includes locking
1862 connectivity to exclusive, managed, and named environments or to a specific set of pre-
1863 approved addresses without user control.

1864 **REFERENCES**

1865 Source Controls: [SC-7\(7\)](#)
1866 Supporting Publications: SP 800-41 [68], SP 800-77 [19], SP 800-189 [71]

1867 **3.13.8. Transmission and Storage Confidentiality**

1868 Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during
1869 transmission and while in storage.

1870 **DISCUSSION**

1871 This requirement applies to internal and external networks and any system components that can
1872 transmit CUI, including servers, notebook computers, desktop computers, mobile devices,

1873 printers, copiers, scanners, facsimile machines, and radios. Communication paths outside of the
1874 physical protection of controlled boundaries are susceptible to both interception and
1875 modification. Encryption protects CUI from unauthorized disclosure during transmission.
1876 Cryptographic mechanisms that protect the confidentiality and integrity of information during
1877 transmission include TLS and IPsec. Cryptographic standards include FIPS-validated
1878 cryptography [30] [31] [32] and NSA-approved cryptography. Information at rest refers to the
1879 state of CUI when it resides on the system and is not in process or in transit, including internal
1880 or external storage devices, storage area network devices, and databases. The focus of
1881 protecting CUI at rest is not on the type of storage device or the frequency of access to that
1882 device but rather on the state of the information.

1883 **REFERENCES**

1884 Source Controls: [SC-8\(1\)](#), [SC-28\(1\)](#)
1885 Supporting Publications: FIPS 140-3 [42], FIPS 197 [72], SP 800-46 [15], SP 800-52 [73], SP
1886 800-56A [77], SP 800-56B [78], SP 800-56C [79], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-
1887 57-3 [18], SP 800-77 [19], SP 800-111 [55], SP 800-113 [20], SP 800-114 [21], SP 800-121
1888 [22], SP 800-124 [29], SP 800-177 [74]

1889 **3.13.9. Network Disconnect**

1890 Terminate network connections associated with communications sessions at the end of the
1891 sessions or after [*Assignment: organization-defined time period*] of inactivity.

1892 **DISCUSSION**

1893 This requirement applies to internal and external networks. Terminating network connections
1894 associated with communications sessions includes de-allocating associated TCP/IP address or
1895 port pairs at the operating system level or de-allocating networking assignments at the
1896 application level if multiple application sessions are using a single operating system-level
1897 network connection. Time periods of user inactivity may be established by organizations and
1898 include time periods by type of network access or for specific network accesses.

1899 **REFERENCES**

1900 Source Controls: [SC-10](#)
1901 Supporting Publications: None

1902 **3.13.10. Cryptographic Key Establishment and Management**

1903 Establish and manage cryptographic keys when cryptography is implemented in the system in
1904 accordance with the following key management requirements: [*Assignment: organization-*
1905 *defined requirements for key generation, distribution, storage, access, and destruction*].

1906 **DISCUSSION**

1907 Cryptographic key management and establishment can be performed using manual procedures
1908 or mechanisms supported by manual procedures. Organizations define key management
1909 requirements in accordance with applicable federal laws, Executive Orders, policies,
1910 directives, regulations, and standards specifying appropriate options, levels, and parameters.

1911 **REFERENCES**

1912 Source Controls: [SC-12](#)

1913 Supporting Publications: FIPS 140-3 [42], SP 800-56A [77], SP 800-56B [78], SP 800-56C
1914 [79], SP 800-57-1 [16], SP 800-57-2 [17], SP 800-57-3 [18], SP 800-63-3 [28]

1915 **3.13.11. Cryptographic Protection**

1916 Implement the following types of cryptography when used to protect the confidentiality of CUI:
1917 [*Assignment: organization-defined types of cryptography*].

1918 **DISCUSSION**

1919 Cryptography can be employed to support a variety of security solutions, including the
1920 protection of CUI. Cryptography is implemented in accordance with applicable laws,
1921 Executive Orders, directives, regulations, policies, standards, and guidelines. FIPS-validated
1922 cryptography is described in [30] [31] [32].

1923 **REFERENCES**

1924 Source Controls: [SC-13](#)
1925 Supporting Publications: FIPS 140-3 [42]

1926 **3.13.12. Collaborative Computing Devices and Applications**

1927 a. Prohibit remote activation of collaborative computing devices and applications with the
1928 following exceptions: [*Assignment: organization-defined exceptions where remote*
1929 *activation is to be allowed*].

1930 b. Provide an explicit indication of use to users physically present at the devices.

1931 **DISCUSSION**

1932 Collaborative computing devices include networked white boards, microphones, and cameras.
1933 Indication of use includes signals to users when collaborative computing devices are activated.
1934 Dedicated video conferencing systems, which rely on one of the participants calling or
1935 connecting to the other party to activate the video conference, are excluded. Solutions to
1936 prevent device usage include webcam covers and buttons to disable microphones.

1937 **REFERENCES**

1938 Source Controls: [SC-15](#)
1939 Supporting Publications: None

1940 **3.13.13. Mobile Code**

1941 a. Define acceptable and unacceptable mobile code and mobile code technologies.

1942 b. Authorize, control, and monitor the use of mobile code.

1943 **DISCUSSION**

1944 Mobile code includes any program, application, or content that can be transmitted across a
1945 network (e.g., embedded in an email, document, or website) and executed on a remote system.
1946 Decisions regarding the use of mobile code within the system are based on the potential for
1947 the code to cause damage to the system if used maliciously. Mobile code technologies include
1948 Java applets, JavaScript, HTML5, VBScript, and WebGL. Usage restrictions and
1949 implementation guidelines apply to the selection and use of mobile code installed on servers

1950 as well as mobile code downloaded and executed on individual workstations and devices,
1951 including notebook computers and smart phones. Mobile code policy and procedures address
1952 the specific actions taken to prevent the development, acquisition, and introduction of
1953 unacceptable mobile code within the system, including requiring mobile code to be digitally
1954 signed by a trusted source.

1955 **REFERENCES**

1956 Source Controls: [SC-18](#)
1957 Supporting Publications: SP 800-28 [75]

1958 **3.13.14.** Withdrawn: Technology-specific.

1959 **3.13.15. Session Authenticity**

1960 Protect the authenticity of communications sessions.

1961 **DISCUSSION**

1962 Protecting session authenticity addresses communications protection at the session level, not
1963 at the packet level. Such protection establishes grounds for confidence at both ends of the
1964 communications sessions in the ongoing identities of other parties and validity of transmitted
1965 information. Authenticity protection includes protecting against “adversary-in-the-middle”
1966 attacks (also known as “man-in-the middle” attacks), session hijacking, and the insertion of
1967 false information into sessions.

1968 **REFERENCES**

1969 Source Controls: [SC-23](#)
1970 Supporting Publications: SP 800-52 [73], SP 800-77 [19], SP 800-95 [76], SP 800-113 [20]

1971 **3.13.16.** Withdrawn: Incorporated into 3.13.8.

1972 **3.13.17. Internal Network Communications Traffic**

1973 Route internal network communications traffic to external networks through an authenticated
1974 proxy server.

1975 **DISCUSSION**

1976 External networks are networks outside of organizational control. A proxy server is a server
1977 (i.e., system or application) that acts as an intermediary for clients who request system
1978 resources from non-organizational or other organizational servers. System resources that may
1979 be requested include files, connections, web pages, or services. Client requests established
1980 through a connection to a proxy server are assessed to manage complexity and provide
1981 additional protection by limiting direct connectivity. Web content filtering devices are one of
1982 the most common proxy servers that provide access to the internet. Proxy servers can support
1983 the logging of Transmission Control Protocol sessions and the blocking of specific Uniform
1984 Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be
1985 configured with organization-defined lists of authorized and unauthorized websites. Note that
1986 proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential

1987 for “adversary-in-the-middle” attacks (also known as “man-in-the middle attacks”) depending
1988 on the implementation.

1989 **REFERENCES**

1990 Source Controls: [SC-7\(8\)](#)

1991 Supporting Publications: SP 800-41 [68], SP 800-125B [69], SP 800-207 [70], SP 800-160-1
1992 [12]

1993 **3.13.18. System Access Points**

1994 Limit the number of external network connections to the system.

1995 **DISCUSSION**

1996 Limiting the number of external network connections facilitates the monitoring of inbound
1997 and outbound communications traffic and is important during transition periods from older to
1998 newer technologies. Such transitions may require implementing older and newer technologies
1999 simultaneously during the transition period and thus increase the number of access points to
2000 the system.

2001 **REFERENCES**

2002 Source Controls: [SC-7\(3\)](#)

2003 Supporting Publications: SP 800-41 [68], SP 800-125B [69], SP 800-207 [70], SP 800-160-1
2004 [12]

2005 **3.14. System and Information Integrity**

2006 **3.14.1. Flaw Remediation**

- 2007 a. Identify, report, and correct system flaws.
- 2008 b. Test software and firmware updates related to flaw remediation for effectiveness and
2009 potential side effects before installation.
- 2010 c. Install security-relevant software and firmware updates within [*Assignment: organization-*
2011 *defined time period*] of the release of the updates.

2012 **DISCUSSION**

2013 Organizations identify systems that are affected by announced software and firmware flaws,
2014 including potential vulnerabilities that result from those flaws, and report this information to
2015 designated personnel with information security responsibilities. Security-relevant updates
2016 include patches, service packs, hot fixes, and anti-virus signatures. Organizations address the
2017 flaws discovered during security assessments, continuous monitoring, incident response
2018 activities, and system error handling. Organizations can take advantage of available resources,
2019 such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures
2020 (CVE) databases, in remediating the flaws discovered in organizational systems. Organization-
2021 defined time periods for updating security-relevant software and firmware may vary based on a
2022 variety of factors, including the criticality of the update (i.e., severity of the vulnerability related
2023 to the discovered flaw). Some types of flaw remediation may require more testing than other
2024 types of remediation.

2025 **REFERENCES**

2026 Source Controls: [SI-2](#)
2027 Supporting Publications: SP 800-39 [64], SP 800-40 [60], SP 800-128 [45]

2028 **3.14.2. Malicious Code Protection**

- 2029 a. Implement malicious code protection mechanisms at designated locations within the system
2030 to detect and eradicate malicious code.
- 2031 b. Update malicious code protection mechanisms as new releases are available in accordance
2032 with organizational configuration management policy and procedures.

2033 **DISCUSSION**

2034 Malicious code insertions occur through the exploitation of system vulnerabilities. Periodic
2035 scans of the system and real-time scans of files from external sources as files are downloaded,
2036 opened, or executed can detect malicious code. Malicious code can be inserted into the system
2037 in a variety of ways, including by electronic mail, the world wide web, and portable storage
2038 devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code
2039 can be encoded in various formats, contained in compressed or hidden files, or hidden in files
2040 using techniques such as steganography. In addition to the above technologies, pervasive
2041 configuration management, comprehensive software integrity controls, and anti-exploitation
2042 software may be effective in preventing the execution of unauthorized code. Malicious code
2043 may be present in commercial off-the-shelf software as well as custom-built software and could
2044 include logic bombs, backdoors, and other types of attacks that could affect organizational
2045 mission and business functions.

2046 In situations where malicious code cannot be detected by detection methods or technologies,
2047 organizations rely on other types of controls – including secure coding practices, configuration
2048 management and control, trusted procurement processes, and monitoring practices – to ensure
2049 that software does not perform functions other than the functions intended. Organizations may
2050 determine that different actions are warranted in response to the detection of malicious code.
2051 For example, organizations can define actions in response to malicious code detection during
2052 scans, the detection of malicious downloads, or the detection of maliciousness when attempting
2053 to open or execute files.

2054 **REFERENCES**

2055 Source Controls: [SI-3](#)
2056 Supporting Publications: SP 800-83 [80], SP 800-125B [69], SP 800-177 [74]

2057 **3.14.3. Security Alerts, Advisories, and Directives**

- 2058 a. Receive security alerts, advisories, and directives from external organizations.
2059 b. Generate internal security alerts, advisories, and directives, as necessary.

2060 **DISCUSSION**

2061 There are many publicly available sources of system security alerts and advisories. For
2062 example, the Department of Homeland Security’s Cybersecurity and Infrastructure Security
2063 Agency (CISA) generates security alerts and advisories to maintain situational awareness across
2064 the Federal Government and in nonfederal organizations. Software vendors, subscription
2065 services, and industry Information Sharing and Analysis Centers (ISACs) may also provide

2066 security alerts and advisories. Compliance with security directives is essential due to the critical
2067 nature of many of these directives and the potential immediate adverse effects on organizational
2068 operations and assets, individuals, other organizations, and the Nation should the directives not
2069 be implemented in a timely manner. Examples of response actions include notifying relevant
2070 external organizations, such as external mission and business partners, supply chain partners,
2071 service providers, and peer or supporting organizations.

2072 **REFERENCES**

2073 Source Controls: [SI-5](#)
2074 Supporting Publications: SP 800-161 [37]

2075 **3.14.4.** Withdrawn: Incorporated into 3.14.2.

2076 **3.14.5.** Withdrawn: Addressed by 3.14.2.

2077 **3.14.6. System Monitoring**

- 2078 a. Monitor the system, including inbound and outbound communications traffic, to detect:
- 2079 1. Attacks and indicators of potential attacks;
- 2080 2. Unusual or unauthorized activities or conditions; and
- 2081 3. Unauthorized connections.
- 2082 b. Identify unauthorized use of the system.

2083 **DISCUSSION**

2084 System monitoring involves external and internal monitoring. External monitoring includes the
2085 observation of events that occur at the system boundary, while internal monitoring includes the
2086 observation of events that occur within the system. Organizations can monitor the system, for
2087 example, by observing audit record activities in real time or by observing other system aspects,
2088 such as access patterns, characteristics of access, and other actions. The monitoring objectives
2089 may guide determination of the events.

2090 A system monitoring capability is achieved through a variety of tools and techniques (e.g., audit
2091 record monitoring software, intrusion detection systems, intrusion prevention systems,
2092 malicious code protection software, scanning tools, network monitoring software). Strategic
2093 locations for monitoring devices include selected perimeter locations and near server farms that
2094 support critical applications with such devices being employed at managed system interfaces.
2095 The granularity of monitoring the information collected is based on organizational monitoring
2096 objectives and the capability of the system to support such objectives.

2097 System monitoring is an integral part of continuous monitoring and incident response programs.
2098 The output from system monitoring serves as input to continuous monitoring and incident
2099 response programs. A network connection is any connection with a device that communicates
2100 through a network (e.g., local area network, internet). A remote connection is any connection
2101 with a device that communicates through an external network (e.g., the internet). Local,
2102 network, and remote connections can be either wired or wireless.

2103 Unusual or unauthorized activities or conditions related to inbound and outbound
2104 communications traffic include internal traffic that indicates the presence of malicious code in
2105 the system or propagating among system components, the unauthorized export of information,

2106 or signaling to external systems. Evidence of malicious code is used to identify a potentially
2107 compromised system. System monitoring requirements, including the need for types of system
2108 monitoring, may be referenced in other requirements.

2109 **REFERENCES**

2110 Source Controls: [SI-4](#), [SI-4\(4\)](#)
2111 Supporting Publications: SP 800-61 [51], SP 800-83 [80], SP 800-92 [39], SP 800-94 [33], SP
2112 800-137 [53], SP 800-177 [74]

2113 **3.14.7.** Withdrawn: Incorporated into 3.14.6.

2114 **3.14.8. Spam Protection**

- 2115 a. Implement spam protection mechanisms at designated locations within the system to detect
2116 and act on unsolicited messages.
2117 b. Update spam protection mechanisms [*Assignment: organization-defined frequency*].

2118 **DISCUSSION**

2119 System entry and exit points include firewalls, remote-access servers, electronic mail servers,
2120 web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can
2121 be transported by different means, including email, email attachments, and web accesses. Spam
2122 protection mechanisms include signature definitions.

2123 **REFERENCES**

2124 Source Controls: [SI-8](#)
2125 Supporting Publications: SP 800-45 [81], SP 800-177 [74]

2126 **3.15. Planning**

2127 **3.15.1. Policy and Procedures**

- 2128 a. Develop, document, and disseminate to organizational personnel or roles, policies and
2129 procedures needed to implement security requirements.
2130 b. Review and update policies and procedures [*Assignment: organization-defined frequency*].

2131 **DISCUSSION**

2132 This requirement addresses policies and procedures for the protection of CUI. Policies and
2133 procedures contribute to security assurance and should address each family of CUI security
2134 requirements. Policies can be included as part of the generalized security policy or be
2135 represented by separate policies that address each family of security requirements. Procedures
2136 describe how policies, requirements, and controls are implemented and can be directed at the
2137 individual or role that is the object of the procedure. Procedures can be documented in system
2138 security plans or in one or more separate documents.

2139 **REFERENCES**

2140 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](#),
2141 [RA-1](#), [SA-1](#), [SC-1](#), [SI-1](#), [SR-1](#)
2142 Supporting Publications: SP 800-12 [65], SP 800-100 [66]

2143 3.15.2. System Security Plan

- 2144 a. Develop and document a system security plan that describes:
- 2145 1. System boundary and operating environment;
- 2146 2. Security requirements, tailoring actions, and implementation; and
- 2147 3. Connections to other systems.
- 2148 b. Review and update the plan at [*Assignment: organization-defined frequency*].

2149 DISCUSSION

2150 System security plans relate security requirements to a set of security controls. System security
2151 plans also provide a high-level description of how the controls meet those requirements but do
2152 not provide detailed descriptions of the design or implementation of the controls. System
2153 security plans contain sufficient information to enable a design and implementation that is
2154 unambiguously compliant with the intent of the plans and the subsequent determinations of risk
2155 if the plan is implemented as intended. System security plans can be a collection of documents,
2156 including documents that already exist. Effective system security plans make use of references
2157 to policies, procedures, and additional documents (e.g., design specifications) where detailed
2158 information can be obtained. This reduces the documentation requirements associated with
2159 security programs and maintains security information in other established management or
2160 operational areas related to enterprise architecture, the system development life cycle, systems
2161 engineering, and acquisition.

2162 REFERENCES

2163 Source Controls: [PL-2](#)

2164 Supporting Publications: SP 800-18 [67]

2165 3.15.3. Rules of Behavior

- 2166 a. Establish and provide to individuals requiring access to the system, the rules that describe
2167 their responsibilities and expected behavior for handling CUI and system usage.
- 2168 b. Review and update the rules of behavior [*Assignment: organization-defined frequency*].

2169 DISCUSSION

2170 Rules of behavior represent a type of access agreement for system users. Organizations consider
2171 rules of behavior for the handling of CUI based on individual user roles and responsibilities and
2172 differentiate between rules that apply to privileged users and rules that apply to general users.

2173 REFERENCES

2174 Source Controls: [PL-4](#)

2175 Supporting Publications: SP 800-18 [67]

2176 3.16. System and Services Acquisition

2177 3.16.1. Security Engineering Principles

2178 Apply systems security engineering principles in the specification, design, development,
2179 implementation, and modification of the system and system components.

2180 **DISCUSSION**

2181 Organizations apply systems security engineering principles to new development systems or
2182 systems undergoing major upgrades. For legacy systems, organizations apply systems security
2183 engineering principles to system upgrades and modifications to the extent feasible, given the
2184 current state of hardware, software, and firmware components within those systems. The
2185 application of systems security engineering concepts and principles helps to develop
2186 trustworthy, secure, and resilient systems and reduce the susceptibility of organizations to
2187 disruptions, hazards, and threats. Examples include developing layered protections; establishing
2188 security policies, architecture, and controls as the foundation for design; incorporating security
2189 requirements into the system development life cycle; delineating physical and logical security
2190 boundaries; ensuring that developers are trained on how to build trustworthy secure software;
2191 and performing threat modeling to identify use cases, threat agents, attack vectors and patterns,
2192 design patterns, and compensating controls needed to mitigate risk. Organizations that apply
2193 security engineering concepts and principles can facilitate the development of trustworthy,
2194 secure systems, system components, and system services; reduce risk to acceptable levels; and
2195 make informed risk-management decisions.

2196 **REFERENCES**

2197 Source Controls: [SA-8](#)
2198 Supporting Publications: SP 800-160-1 [12], SP 800-160-2 [11], SP 800-207 [70]

2199 **3.16.2. Unsupported System Components**

- 2200 a. Replace system components when support for the components is no longer available from
2201 the developer, vendor, or manufacturer; or
2202 b. Provide options for alternative sources for continued support for unsupported components.

2203 **DISCUSSION**

2204 Support for system components includes software patches, firmware updates, replacement parts,
2205 and maintenance contracts. An example of unsupported components includes when vendors no
2206 longer provide critical software patches or product updates, which can result in an opportunity
2207 for adversaries to exploit weaknesses in the installed components. Exceptions to replacing
2208 unsupported system components include systems that provide critical mission or business
2209 capabilities where newer technologies are not available or where the systems are so isolated that
2210 installing replacement components is not an option.

2211 Alternative sources for support address the need to provide continued support for system
2212 components that are no longer supported by the original manufacturers, developers, or vendors
2213 when such components remain essential to organizational mission and business functions. If
2214 necessary, organizations can establish in-house support by developing customized patches for
2215 critical software components or, alternatively, obtain the services of external providers who
2216 provide ongoing support for the designated unsupported components through contractual
2217 relationships. Such contractual relationships can include open-source software value-added
2218 vendors. The increased risk of using unsupported system components can be mitigated, for
2219 example, by prohibiting the connection of such components to public or uncontrolled networks
2220 or implementing other forms of isolation.

2221 **REFERENCES**

2222 Source Controls: [SA-22](#)
2223 Supporting Publications: None

2224 3.16.3. External System Services

- 2225 a. Require the providers of external system services to comply with organizational security
2226 requirements, and implement the following controls: [*Assignment: organization-defined*
2227 *controls*].
- 2228 b. Define and document organizational oversight and user roles and responsibilities with
2229 regard to external system services.
- 2230 c. Implement the following processes, methods, and techniques to monitor control compliance
2231 by external service providers on an ongoing basis: [*Assignment: organization-defined*
2232 *processes, methods, and techniques*].

2233 DISCUSSION

2234 External system services are provided by an external provider, and in most cases, the
2235 organization has no direct control over the implementation of the required controls or the
2236 assessment of control effectiveness. Organizations establish relationships with external service
2237 providers in a variety of ways, including through business partnerships, contracts, interagency
2238 agreements, lines of business arrangements, licensing agreements, joint ventures, and supply
2239 chain exchanges. The responsibility for managing risks from the use of external system services
2240 remains with the organization charged with protecting CUI. Service-level agreements define the
2241 expectations of performance for the implemented controls, describe measurable outcomes, and
2242 identify remedies, mitigations, and response requirements for identified instances of
2243 noncompliance. Information from external service providers regarding the specific functions,
2244 ports, protocols, and services used in the provision of such services can be useful when the need
2245 arises to understand the trade-offs involved in restricting certain functions and services or
2246 blocking certain ports and protocols.

2247 REFERENCES

2248 Source Controls: [SA-9](#)
2249 Supporting Publications: SP 800-160-1 [12], SP 800-161 [37]

2250 3.17. Supply Chain Risk Management

2251 3.17.1. Supply Chain Risk Management Plan

- 2252 a. Develop a plan for managing supply chain risks associated with the development,
2253 manufacturing, acquisition, delivery, operations, maintenance, and disposal of the system,
2254 system components, or system services.
- 2255 b. Review and update the plan [*Assignment: organization-defined frequency*].

2256 DISCUSSION

2257 Dependence on the products, systems, and services from external providers and the nature of the
2258 relationships with those providers present an increasing level of risk to an organization. Threat
2259 actions that may increase security risks include unauthorized production, the insertion or use of
2260 counterfeits, tampering, theft, insertion of malicious software and hardware, and poor
2261 manufacturing and development practices in the supply chain. Supply chain risks can be endemic
2262 or systemic within a system, component, or service. Managing supply chain risk is a complex,
2263 multifaceted undertaking that requires a coordinated effort across an organization to build trust
2264 relationships and communicate with internal and external stakeholders.

2265 Supply chain risk management (SCRM) activities include identifying and assessing risks,
2266 determining appropriate risk response actions, developing SCRM plans to document response
2267 actions, and monitoring performance against plans. The system-level SCRM plan is
2268 implementation-specific and provides policy implementation, requirements, constraints and
2269 implications. It can either be stand-alone or incorporated into system security plans. The SCRM
2270 plan addresses the management, implementation, and monitoring of SCRM controls and the
2271 development or sustainment of systems across the SDLC to support mission and business
2272 functions. Because supply chains can differ significantly across and within organizations, SCRM
2273 plans are tailored to individual program, organizational, and operational contexts.

2274 **REFERENCES**

2275 Source Controls: [SR-2](#)
2276 Supporting Publications: SP 800-30 [59], SP 800-39 [64], SP 800-160-1 [12], SP 800-181 [38]

2277 **3.17.2. Acquisition Strategies, Tools, and Methods**

2278 Develop and implement acquisition strategies, contract tools, and procurement methods to
2279 protect against, identify, and mitigate supply chain risks.

2280 **DISCUSSION**

2281 The acquisition process provides an important vehicle for protecting the supply chain. There are
2282 many useful tools and techniques available, including obscuring the end use of a system or
2283 system component, using blind or filtered buys, requiring tamper-evident packaging, or using
2284 trusted or controlled distribution. The results from a supply chain risk assessment can inform
2285 the strategies, tools, and methods that are most applicable to the situation. Tools and techniques
2286 may provide protections against unauthorized production, theft, tampering, the insertion of
2287 counterfeits, the insertion of malicious software or backdoors, and poor development practices
2288 throughout the system life cycle.

2289 Organizations also consider providing incentives for suppliers to implement controls, promote
2290 transparency in their processes and security practices, provide contract language that addresses
2291 the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy
2292 suppliers. Organizations consider providing training, education, and awareness programs for
2293 personnel regarding supply chain risk, available mitigation strategies, and when the programs
2294 should be employed. Methods for reviewing and protecting development plans, documentation,
2295 and evidence are commensurate with the security requirements of the organization. Contracts
2296 may specify documentation protection requirements.

2297 **REFERENCES**

2298 Source Controls: [SR-5](#)
2299 Supporting Publications: SP 800-30 [59], SP 800-161 [37]

2300 **3.17.3. Supply Chain Controls and Processes**

- 2301 a. Establish a process or processes for identifying and addressing weaknesses or deficiencies
2302 in the supply chain elements and processes.
- 2303 b. Employ the following controls to protect against supply chain risks to the system, system
2304 component, or system service and to limit the harm or consequences from supply chain-
2305 related events: [*Assignment: organization-defined supply chain controls*].

2306

DISCUSSION

2307

2308

2309

2310

2311

2312

2313

2314

2315

2316

2317

2318

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.

2319

REFERENCES

2320

Source Controls: [SR-3](#)

2321

Supporting Publications: SP 800-30 [59], SP 800-161 [37]

2322

3.17.4. Component Disposal

2323

2324

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

2325

DISCUSSION

2326

2327

2328

2329

2330

2331

2332

2333

2334

2335

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.

2336

REFERENCES

2337

Source Controls: [SR-12](#)

2338

Supporting Publications: SP 800-30 [59], SP 800-161 [37]

2339 **References**

- 2340 [1] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House,
2341 Washington, DC), DCPD-201000942, November 4, 2010. Available at
2342 <https://www.govinfo.gov/app/details/DCPD-201000942>
- 2343 [2] Executive Order 13526 (2009) Classified National Security Information. (The White House,
2344 Washington, DC), DCPD-200901022, December 29, 2009. Available at
2345 <https://www.govinfo.gov/app/details/DCPD-200901022>
- 2346 [3] Atomic Energy Act (P.L. 83-703), August 1954. Available at
2347 <https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919>
- 2348 [4] National Archives and Records Administration (2019) Controlled Unclassified Information
2349 (CUI) Registry. Available at <https://www.archives.gov/cui>
- 2350 [5] 32 CFR Part 2002 (2016), Controlled Unclassified Information (CUI), September 2016.
2351 Available at <https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018->
2352 [title32-vol6-part2002.pdf](https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf)
- 2353 [6] National Institute of Standards and Technology (2004) Standards for Security
2354 Categorization of Federal Information and Information Systems. (U.S. Department of
2355 Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS)
2356 199. <https://doi.org/10.6028/NIST.FIPS.199>
- 2357 [7] National Institute of Standards and Technology (2006) Minimum Security Requirements for
2358 Federal Information and Information Systems. (U.S. Department of Commerce,
2359 Washington, DC), Federal Information Processing Standards Publication (FIPS) 200.
2360 <https://doi.org/10.6028/NIST.FIPS.200>
- 2361 [8] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for
2362 Information Systems and Organizations. (National Institute of Standards and Technology,
2363 Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of
2364 December 10, 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>
- 2365 [9] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available
2366 at <https://www.govinfo.gov/app/details/PLAW-113publ283>
- 2367 [10] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial
2368 Control Systems (ICS) Security. (National Institute of Standards and Technology,
2369 Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2.
2370 <https://doi.org/10.6028/NIST.SP.800-82r2>
- 2371 [11] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-
2372 Resilient Systems: A Systems Security Engineering Approach. (National Institute of
2373 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160,
2374 Vol. 2, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- 2375 [12] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems.
2376 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2377 Publication (SP) 800-160, Vol. 1, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-160v1r1>
- 2378 [13] Joint Task Force Transformation Initiative (2020) Control Baselines for Systems and
2379 Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2380 Special Publication (SP) 800-53B, Includes updates as of December 10, 2020.
2381 <https://doi.org/10.6028/NIST.SP.800-53B>

- 2382 [14] Office of Management and Budget Memorandum Circular A-130, Managing Information as
2383 a Strategic Resource, July 2016. Available at [https://www.whitehouse.gov/wp-
content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf](https://www.whitehouse.gov/wp-
2384 content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)
- 2385 [15] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and
2386 Bring Your Own Device (BYOD) Security. (National Institute of Standards and
2387 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2.
2388 <https://doi.org/10.6028/NIST.SP.800-46r2>
- 2389 [16] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National
2390 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2391 800-57 Part 1, Rev. 5. <https://doi.org/10.6028/NIST.SP.800-57pt1r5>
- 2392 [17] Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best
2393 Practices for Key Management Organizations. (National Institute of Standards and
2394 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1.
2395 <https://doi.org/10.6028/NIST.SP.800-57pt2r1>
- 2396 [18] Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-
2397 Specific Key Management Guidance. (National Institute of Standards and Technology,
2398 Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1.
2399 <https://doi.org/10.6028/NIST.SP.800-57pt3r1>
- 2400 [19] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs.
2401 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2402 Publication (SP) 800-77, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-77r1>
- 2403 [20] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National
2404 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2405 800-113. <https://doi.org/10.6028/NIST.SP.800-113>
- 2406 [21] Souppaya MP, Scarfone KA (2016) User’s Guide to Telework and Bring Your Own Device
2407 (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD),
2408 NIST Special Publication (SP) 800-114, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-114r1>
- 2409 [22] Padgett J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide
2410 to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD),
2411 NIST Special Publication (SP) 800-121, Rev. 2, Includes updates as of January 19, 2022.
2412 <https://doi.org/10.6028/NIST.SP.800-121r2-upd1>
- 2413 [23] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014)
2414 Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National
2415 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2416 800-162, Includes updates as of August 2, 2019. <https://doi.org/10.6028/NIST.SP.800-162>
- 2417 [24] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based
2418 Access Control (ABAC) Standards for Data Service Applications: Extensible Access
2419 Control Markup Language (XACML) and Next Generation Access Control (NGAC).
2420 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2421 Publication (SP) 800-178. <https://doi.org/10.6028/NIST.SP.800-178>
- 2422 [25] Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control
2423 Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2424 Special Publication (SP) 800-192. <https://doi.org/10.6028/NIST.SP.800-192>

- 2425 [26] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics.
2426 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or
2427 Internal Report (IR) 7874. <https://doi.org/10.6028/NIST.IR.7874>
- 2428 [27] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and
2429 Automated Access Management Using Secure Shell (SSH). (National Institute of Standards
2430 and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966.
2431 <https://doi.org/10.6028/NIST.IR.7966>
- 2432 [28] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of
2433 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3,
2434 Includes updates as of March 2, 2020. <https://doi.org/10.6028/NIST.SP.800-63-3>
- 2435 [29] Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile
2436 Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg,
2437 MD), NIST Special Publication (SP) 800-124, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-124r1>
- 2438
- 2439 [30] National Institute of Standards and Technology (2019) Cryptographic Standards and
2440 Guidelines. Available at [https://csrc.nist.gov/projects/cryptographic-standards-and-](https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines)
2441 [guidelines](https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines)
- 2442 [31] National Institute of Standards and Technology (2019) Cryptographic Algorithm Validation
2443 Program. Available at <https://csrc.nist.gov/projects/cavp>
- 2444 [32] National Institute of Standards and Technology (2019) Cryptographic Module Validation
2445 Program. Available at <https://csrc.nist.gov/projects/cmvp>
- 2446 [33] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems
2447 (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2448 Publication (SP) 800-94. <https://doi.org/10.6028/NIST.SP.800-94>
- 2449 [34] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security
2450 Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology,
2451 Gaithersburg, MD), NIST Special Publication (SP) 800-97.
2452 <https://doi.org/10.6028/NIST.SP.800-97>
- 2453 [35] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device
2454 (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD),
2455 NIST Special Publication (SP) 800-114, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-114r1>
- 2456 [36] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and
2457 Training Program. (National Institute of Standards and Technology, Gaithersburg, MD),
2458 NIST Special Publication (SP) 800-50. <https://doi.org/10.6028/NIST.SP.800-50>
- 2459 [37] Boyens JM, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity
2460 Supply Chain Risk Management Practices for Systems and Organizations. (National
2461 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2462 800-161, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-161r1>
- 2463 [38] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for
2464 Cybersecurity (NICE Framework). (National Institute of Standards and Technology,
2465 Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1.
2466 <https://doi.org/10.6028/NIST.SP.800-181r1>
- 2467 [39] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National
2468 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2469 800-92. <https://doi.org/10.6028/NIST.SP.800-92>

- 2470 [40] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques
2471 into Incident Response. (National Institute of Standards and Technology, Gaithersburg,
2472 MD), NIST Special Publication (SP) 800-86. <https://doi.org/10.6028/NIST.SP.800-86>
- 2473 [41] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National
2474 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2475 800-101, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-101r1>
- 2476 [42] National Institute of Standards and Technology (2019) Security Requirements for
2477 Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal
2478 Information Processing Standards Publication (FIPS) 140-3.
2479 <https://doi.org/10.6028/NIST.FIPS.140-3>
- 2480 [43] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S.
2481 Department of Commerce, Washington, D.C.), Federal Information Processing Standards
2482 Publication (FIPS) 180-4. <https://doi.org/10.6028/NIST.FIPS.180-4>
- 2483 [44] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based
2484 Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington,
2485 D.C.), Federal Information Processing Standards Publication (FIPS) 202.
2486 <https://doi.org/10.6028/NIST.FIPS.202>
- 2487 [45] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused
2488 Configuration Management of Information Systems. (National Institute of Standards and
2489 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates
2490 as of October 10, 2019. <https://doi.org/10.6028/NIST.SP.800-128>
- 2491 [46] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control
2492 Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and
2493 Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2.
2494 <https://doi.org/10.6028/NIST.IR.8011-2>
- 2495 [47] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control
2496 Assessments: Volume 3: Software Asset Management. (National Institute of Standards and
2497 Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3.
2498 <https://doi.org/10.6028/NIST.IR.8011-3>
- 2499 [48] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for
2500 IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards
2501 and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4.
2502 <https://doi.org/10.6028/NIST.SP.800-70r4>
- 2503 [49] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical
2504 Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3.
2505 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2506 Publication (SP) 800-126, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-126r3>
- 2507 [50] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting.
2508 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2509 Publication (SP) 800-167. <https://doi.org/10.6028/NIST.SP.800-167>
- 2510 [51] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident
2511 Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2512 Special Publication (SP) 800-61, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-61r2>

- 2513 [52] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training,
2514 and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and
2515 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84.
2516 <https://doi.org/10.6028/NIST.SP.800-84>
- 2517 [53] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA,
2518 Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal
2519 Information Systems and Organizations. (National Institute of Standards and Technology,
2520 Gaithersburg, MD), NIST Special Publication (SP) 800-137.
2521 <https://doi.org/10.6028/NIST.SP.800-137>
- 2522 [54] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media
2523 Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2524 Special Publication (SP) 800-88, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-88r1>
- 2525 [55] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies
2526 for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD),
2527 NIST Special Publication (SP) 800-111. <https://doi.org/10.6028/NIST.SP.800-111>
- 2528 [56] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning
2529 Guide for Federal Information Systems. (National Institute of Standards and Technology,
2530 Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of
2531 November 11, 2010. <https://doi.org/10.6028/NIST.SP.800-34r1>
- 2532 [57] Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing
2533 Cryptographic Key Management Systems. (National Institute of Standards and Technology,
2534 Gaithersburg, MD), NIST Special Publication (SP) 800-130.
2535 <https://doi.org/10.6028/NIST.SP.800-130>
- 2536 [58] Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key
2537 Management Systems (CKMS). (National Institute of Standards and Technology,
2538 Gaithersburg, MD), NIST Special Publication (SP) 800-152.
2539 <https://doi.org/10.6028/NIST.SP.800-152>
- 2540 [59] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments.
2541 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2542 Publication (SP) 800-30, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- 2543 [60] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning:
2544 Preventive Maintenance for Technology. (National Institute of Standards and Technology,
2545 Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4.
2546 <https://doi.org/10.6028/NIST.SP.800-40r4>
- 2547 [61] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls
2548 in Information Systems and Organizations. (National Institute of Standards and Technology,
2549 Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5.
2550 <https://doi.org/10.6028/NIST.SP.800-53Ar5>
- 2551 [62] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information
2552 Security Testing and Assessment. (National Institute of Standards and Technology,
2553 Gaithersburg, MD), NIST Special Publication (SP) 800-115.
2554 <https://doi.org/10.6028/NIST.SP.800-115>

- 2555 [63] Joint Task Force (2018) Risk Management Framework for Information Systems and
2556 Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute
2557 of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37,
2558 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- 2559 [64] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:
2560 Organization, Mission, and Information System View. (National Institute of Standards and
2561 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
2562 <https://doi.org/10.6028/NIST.SP.800-39>
- 2563 [65] Nieves M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security.
2564 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2565 Publication (SP) 800-12, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-12r1>
- 2566 [66] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers.
2567 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2568 Publication (SP) 800-100, Includes updates as of March 7, 2007.
2569 <https://doi.org/10.6028/NIST.SP.800-100>
- 2570 [67] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal
2571 Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD),
2572 NIST Special Publication (SP) 800-18, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-18r1>
- 2573 [68] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National
2574 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2575 800-41, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-41r1>
- 2576 [69] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM)
2577 Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2578 Special Publication (SP) 800-125B. <https://doi.org/10.6028/NIST.SP.800-125B>
- 2579 [70] Rose S, Borchert O, Mitchell S, Connelly S (2017) Zero Trust Architecture. (National
2580 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2581 800-207. <https://doi.org/10.6028/NIST.SP.800-207>
- 2582 [71] Sriram K, Montgomery D (2019) Resilient Interdomain Traffic Exchange: BGP Security
2583 and DDoS Mitigation. (National Institute of Standards and Technology, Gaithersburg, MD),
2584 NIST Special Publication (SP) 800-189. <https://doi.org/10.6028/NIST.SP.800-189>
- 2585 [72] National Institute of Standards and Technology (2001) Advanced Encryption Standard
2586 (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing
2587 Standards Publication (FIPS) 197. <https://doi.org/10.6028/NIST.FIPS.197>
- 2588 [73] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of
2589 Transport Layer Security (TLS) Implementations. (National Institute of Standards and
2590 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2.
2591 <https://doi.org/10.6028/NIST.SP.800-52r2>
- 2592 [74] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email.
2593 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2594 Publication (SP) 800-177, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-177r1>
- 2595 [75] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile
2596 Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2597 Publication (SP) 800-28, Version 2. <https://doi.org/10.6028/NIST.SP.800-28ver2>

- 2598 [76] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National
2599 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2600 800-95. <https://doi.org/10.6028/NIST.SP.800-95>
- 2601 [77] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-
2602 Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National
2603 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2604 800-56A, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>
- 2605 [78] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation
2606 for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National
2607 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2608 800-56B, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-56Br2>
- 2609 [79] Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-
2610 Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg,
2611 MD), NIST Special Publication (SP) 800-56C, Rev. 2.
2612 <https://doi.org/10.6028/NIST.SP.800-56Cr2>
- 2613 [80] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for
2614 Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD),
2615 NIST Special Publication (SP) 800-83, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-83r1>
- 2616 [81] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail
2617 Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2618 Special Publication (SP) 800-45, Version 2. <https://doi.org/10.6028/NIST.SP.800-45ver2>
- 2619 [82] Committee on National Security Systems (2015) Committee on National Security Systems
2620 (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS
2621 Instruction 4009. Available at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- 2622 [83] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. Available at
2623 [https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-
chap35-subchapII-sec3552](https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-
2624 chap35-subchapII-sec3552)
- 2625 [84] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards.
2626 2017 ed. Available at [https://www.govinfo.gov/app/details/USCODE-2017-
title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331](https://www.govinfo.gov/app/details/USCODE-2017-
2627 title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331)
- 2628 [85] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at
2629 [https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-
chap35-subchapI-sec3502](https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-
2630 chap35-subchapI-sec3502)
- 2631 [86] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide.
2632 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2633 Publication (SP) 800-81-2. <https://doi.org/10.6028/NIST.SP.800-81-2>
- 2634 [87] Dempsey K, Pillitteri V, Regenscheid A (2021) Managing the Security of Information
2635 Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2636 Special Publication (SP) 800-47, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-47r1>

2637 **Appendix A. Acronyms**

2638 **BYOD**

2639 Bring Your Own Device

2640 **CFR**

2641 Code of Federal Regulations

2642 **CISA**

2643 Cybersecurity and Infrastructure Security Agency

2644 **CNSS**

2645 Committee on National Security Systems

2646 **CUI**

2647 Controlled Unclassified Information

2648 **CVE**

2649 Common Vulnerabilities and Exposures

2650 **CVSS**

2651 Common Vulnerabilities Scoring System

2652 **CWE**

2653 Common Weakness Enumeration

2654 **DMZ**

2655 Demilitarized Zone

2656 **EAP**

2657 Extensible Authentication Protocol

2658 **EO**

2659 Executive Order

2660 **FIPS**

2661 Federal Information Processing Standards

2662 **FISMA**

2663 Federal Information Security Modernization Act

2664 **FOIA**

2665 Freedom of Information Act

2666 **FTP**

2667 File Transfer Protocol

2668 **GMT**

2669 Greenwich Mean Time

2670 **IEEE**

2671 Institute of Electrical and Electronics Engineers

2672 **IoT**

2673 Internet of Things

2674	ISOO
2675	Information Security Oversight Office
2676	IT
2677	Information Technology
2678	ITL
2679	Information Technology Laboratory
2680	LSI
2681	Large-Scale Integration
2682	MAC
2683	Media Access Control
2684	NARA
2685	National Archives and Records Administration
2686	NFO
2687	Nonfederal Organization
2688	NIST
2689	National Institute of Standards and Technology
2690	NVD
2691	National Vulnerabilities Database
2692	ODP
2693	Organization-Defined Parameter
2694	OMB
2695	Office of Management and Budget
2696	OT
2697	Operational Technology
2698	PII
2699	Personally Identifiable Information
2700	PIN
2701	Personal Identification Number
2702	PROM
2703	Programmable Read-Only Memory
2704	ROM
2705	Read-Only Memory
2706	SCAP
2707	Security Content Automation Protocol
2708	SCRM
2709	Supply Chain Risk Management

- 2710 **SDLC**
- 2711 System Development Life Cycle

- 2712 **SP**
- 2713 Special Publication

- 2714 **TCP/IP**
- 2715 Transmission Control Protocol/Internet Protocol

- 2716 **TLS**
- 2717 Transport Layer Security

- 2718 **UTC**
- 2719 Coordinated Universal Time

- 2720 **VPN**
- 2721 Virtual Private Network

2722 **Appendix B. Glossary**

2723 Appendix B provides definitions for the terminology used in NIST SP 800-171. The definitions
2724 are consistent with the definitions contained in the National Information Assurance Glossary [82]
2725 unless otherwise noted.

2726 **agency**

2727 Any executive agency or department, military department, Federal Government corporation, Federal Government-
2728 controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any
2729 independent regulatory agency. [14]

2730 **assessment**

2731 See *security control assessment*.

2732 **assessor**

2733 See *security control assessor*.

2734 **audit log**

2735 A chronological record of system activities, including records of system accesses and operations performed in a
2736 given period.

2737 **audit record**

2738 An individual entry in an audit log related to an audited event.

2739 **authentication**

2740 Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a
2741 system. Adapted from [7]

2742 **availability**

2743 Ensuring timely and reliable access to and use of information. [83]

2744 **advanced persistent threat**

2745 An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create
2746 opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and
2747 deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the
2748 targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a
2749 mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced
2750 persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it;
2751 and is determined to maintain the level of interaction needed to execute its objectives. [64]

2752 **baseline configuration**

2753 A documented set of specifications for a system or a configuration item within a system that has been formally
2754 reviewed and agreed on at a given point in time, and that can be changed only through change control procedures.

2755 **confidentiality**

2756 Preserving authorized restrictions on information access and disclosure, including means for protecting personal
2757 privacy and proprietary information. [83]

2758 **configuration management**

2759 A collection of activities focused on establishing and maintaining the integrity of information technology products
2760 and systems through control of processes for initializing, changing, and monitoring the configurations of those
2761 products and systems throughout the system development life cycle.

2762 **configuration settings**

2763 The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or
2764 functionality of the system.

2765 **controlled area**

2766 Any area or space for which the organization has confidence that the physical and procedural protections provided
2767 are sufficient to meet the requirements established for protecting the information or system.

2768 **controlled unclassified information**

2769 Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls,
2770 excluding information that is classified under Executive Order 13526, Classified National Security Information,
2771 December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [1]

2772 **CUI Executive Agent**

2773 The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI
2774 Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this
2775 authority to the Director of the Information Security Oversight Office (ISOO). [5]

2776 **CUI program**

2777 The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the
2778 rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI
2779 Registry. [5]

2780 **CUI registry**

2781 The online repository for all information, guidance, policy, and requirements on handling CUI, including everything
2782 issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry
2783 identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls,
2784 establishes markings, and includes guidance on handling procedures. [5]

2785 **cyber-physical systems**

2786 Interacting digital, analog, physical, and human components engineered for function through integrated physics and
2787 logic.

2788 **executive agency**

2789 An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an
2790 independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully
2791 subject to the provisions of 31 U.S.C. Chapter 91.

2792 **external system (or component)**

2793 A system or component of a system that is outside of the authorization boundary established by the organization and
2794 for which the organization typically has no direct control over the application of required security controls or the
2795 assessment of security control effectiveness.

2796 **external system service**

2797 A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a
2798 service that is used by, but not a part of, the organizational system) and for which the organization typically has no
2799 direct control over the application of required security controls or the assessment of security control effectiveness.

2800 **external network**

2801 A network not controlled by the organization.

2802 **federal agency**

2803 See *executive agency*.

2804 **federal information system**

2805 An information system used or operated by an executive agency, by a contractor of an executive agency, or by
2806 another organization on behalf of an executive agency. [84]

2807 **FIPS-validated cryptography**

2808 A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements
2809 specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module
2810 is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by
2811 the Cryptographic Algorithm Validation Program (CAVP). See *NSA-approved cryptography*.

2812 **firmware**

2813 Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-
2814 only memory (PROM) – such that the programs and data cannot be dynamically written or modified during
2815 execution of the programs. See *hardware* and *software*. [82]

2816 **hardware**

2817 The material physical components of a system. See *software* and *firmware*. [82]

2818 **identifier**

2819 Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples
2820 of identifiers.

2821 A unique label used by a system to indicate a specific entity, object, or group.

2822 **impact**

2823 With respect to security, the effect on organizational operations, organizational assets, individuals, other
2824 organizations, or the Nation (including the national security interests of the United States) of a loss of
2825 confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that
2826 individuals could experience when an information system processes their PII.

2827 **impact value**

2828 The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or
2829 availability of information expressed as a value of low, moderate or high. [6]

2830 **incident**

2831 An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or
2832 availability of information or an information system; or constitutes a violation or imminent threat of violation of
2833 law, security policies, security procedures, or acceptable use policies. [83]

2834 **information**

2835 Any communication or representation of knowledge such as facts, data, or opinions in any medium or form,
2836 including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [14]

2837 **information flow control**

2838 Procedure to ensure that information transfers within a system do not violate the security policy.

2839 **information resources**

2840 Information and related resources, such as personnel, equipment, funds, and information technology. [85]

2841 **information security**

2842 The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or
2843 destruction in order to provide confidentiality, integrity, and availability. [83]

2844 **information system**

2845 A discrete set of information resources organized for the collection, processing, maintenance, use, sharing,
2846 dissemination, or disposition of information. [85]

2847 **information technology**

2848 Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic
2849 acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching,
2850 interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such
2851 services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that
2852 requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product.
2853 Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and
2854 storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the
2855 central processing unit of a computer, software, firmware and similar procedures, services (including cloud
2856 computing and help-desk services or other professional services which support any point of the life cycle of the
2857 equipment or service), and related resources. Information technology does not include any equipment that is
2858 acquired by a contractor incidental to a contract which does not require its use. [14]

2859 **insider threat**

2860 The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of
2861 the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized
2862 disclosure, or through the loss or degradation of departmental resources or capabilities.

2863 **integrity**

2864 Guarding against improper information modification or destruction and includes ensuring information non-
2865 repudiation and authenticity. [83]

2866 **internal network**

2867 A network where the establishment, maintenance, and provisioning of security controls are under the direct control
2868 of organizational employees or contractors; or the cryptographic encapsulation or similar security technology
2869 implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and
2870 integrity). An internal network is typically organization-owned yet may be organization-controlled while not being
2871 organization-owned.

2872 **least privilege**

2873 The principle that a security architecture is designed so that each entity is granted the minimum system
2874 authorizations and resources needed to perform its function.

2875 **malicious code**

2876 Software or firmware intended to perform an unauthorized process that will have an adverse impact on the
2877 confidentiality, integrity, or availability of a system. Examples of malicious code include viruses, worms, Trojan
2878 horses, spyware, some forms of adware, or other code-based entities that infect a host.

2879 **media**

2880 Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks,
2881 Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which
2882 information is recorded, stored, or printed within a system. [7]

2883 **mobile code**

2884 Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed
2885 on a local system without explicit installation or execution by the recipient.

2886 **mobile device**

2887 A portable computing device that has a small form factor such that it can easily be carried by a single individual; is
2888 designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local,
2889 non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also
2890 include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in
2891 features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.

2892 **multi-factor authentication**

2893 Authentication using two or more different factors to achieve authentication. Factors include something you know
2894 (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are
2895 (e.g., biometric). See *authenticator*.

2896 **network**

2897 A system implemented with a collection of interconnected components. Such components may include routers,
2898 hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

2899 **network access**

2900 Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local
2901 area network, wide area network, the internet).

2902 **nonfederal organization**

2903 An entity that owns, operates, or maintains a nonfederal system.

2904 **nonfederal system**

2905 A system that does not meet the criteria for a federal system.

2906 **nonlocal maintenance**

2907 Maintenance activities conducted by individuals communicating through a network, either an external network (e.g.,
2908 the internet) or an internal network.

2909 **on behalf of (an agency)**

2910 A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains
2911 or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those
2912 activities are not incidental to providing a service or product to the government. [5]

2913 **organization**

2914 An entity of any size, complexity, or positioning within an organizational structure. Adapted from [7]

2915 **overlay**

2916 A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting
2917 information employed during the tailoring process, that is intended to complement (and further refine) security
2918 control baselines. The overlay specification may be more stringent or less stringent than the original security control
2919 baseline specification and can be applied to multiple information systems. [14]

2920 **personnel security**

2921 The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties
2922 and responsibilities requiring trustworthiness. [8]

2923 **portable storage device**

2924 A system component that can be inserted into and removed from a system, and that is used to store data or
2925 information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic,
2926 optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk
2927 drives, flash memory cards/drives that contain nonvolatile memory).

2928 **potential impact**

2929 The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS
2930 Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic
2931 adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals. [6]

2932 **privileged account**

2933 A system account with authorizations of a privileged user.

- 2934 **privileged user**
2935 A user who is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not
2936 authorized to perform.
- 2937 **records**
2938 The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms,
2939 reports, test results) that serve as a basis for verifying that the organization and the system are performing as
2940 intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a
2941 program and that contain the complete set of information on particular items).
- 2942 **remote access**
2943 Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an
2944 external network (e.g., the internet). Remote access methods include dial-up, broadband, and wireless.
- 2945 **remote maintenance**
2946 Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).
- 2947 **replay resistant**
2948 Protection against the capture of transmitted authentication or access control information and its subsequent
2949 retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
- 2950 **risk**
2951 A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a
2952 function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
2953 (ii) the likelihood of occurrence. [14]
- 2954 **risk assessment**
2955 The process of identifying risks to organizational operations (including mission, functions, image, reputation),
2956 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. [59]
- 2957 **sanitization**
2958 Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization,
2959 extraordinary means.
- 2960 Process to remove information from media such that data recovery is not possible. It includes removing all classified
2961 labels, markings, and activity logs.
- 2962 **security**
2963 A condition that results from the establishment and maintenance of protective measures that enable an organization
2964 to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures
2965 may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should
2966 form part of the organization's risk management approach. [82]
- 2967 **security assessment**
2968 See *security control assessment*.
- 2969 **security control**
2970 The safeguards or countermeasures prescribed for an information system or an organization to protect the
2971 confidentiality, integrity, and availability of the system and its information. [14]
- 2972 **security control assessment**
2973 The testing or evaluation of security controls to determine the extent to which the controls are implemented
2974 correctly, operating as intended, and producing the desired outcome with respect to meeting the security
2975 requirements for an information system or organization. [14]

- 2976 **security domain**
2977 A domain that implements a security policy and is administered by a single authority. Adapted from [82]
- 2978 **security functions**
2979 The hardware, software, or firmware of the system responsible for enforcing the system security policy and
2980 supporting the isolation of code and data on which the protection is based.
- 2981 **split tunneling**
2982 The process of allowing a remote user or device to establish a non-remote connection with a system and
2983 simultaneously communicate via some other connection to a resource in an external network. This method of
2984 network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing
2985 uncontrolled networks.
- 2986 **system**
2987 See *information system*.
- 2988 **system component**
2989 A discrete identifiable information technology asset that represents a building block of a system and may include
2990 hardware, software, and firmware. [45]
- 2991 **system security plan**
2992 A document that describes how an organization meets the security requirements for a system or plans to meet the
2993 requirements. In particular, the system security plan describes the system boundary; the environment in which the
2994 system operates; how the security requirements are implemented; and the relationships with or connections to other
2995 systems.
- 2996 **system service**
2997 A capability provided by a system that facilitates information processing, storage, or transmission.
- 2998 **threat**
2999 Any circumstance or event with the potential to adversely impact organizational operations, organizational assets,
3000 individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure,
3001 modification of information, and/or denial of service. [59]
- 3002 **system user**
3003 An individual, or (system) process acting on behalf of an individual that is authorized to access a system.

3004 **Appendix C. Tailoring Criteria**

3005 This appendix lists the security controls in the NIST SP 800-53 moderate baseline [13]. The
 3006 symbols in [Table 2](#) are used in [Table 3](#) through [Table 22](#) to specify the tailoring actions taken to
 3007 obtain the security requirements in [Section 3](#). The security controls and control enhancements in
 3008 the tables below are hyperlinked to the NIST [Cybersecurity and Privacy Reference Tool](#), which
 3009 provides online access to the specific control language and supplemental materials in NIST SP
 3010 800-53.

3011 **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

3012

3013 **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	3.1.3.8
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

3014

3015

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	—

3016

3017

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

3018

3019

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

3020

3021

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	—

3022

3023

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

3027

3028

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	—

3029

3030

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

3031

3032

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

3033

Table 14. [Planning](#)

3034

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	—

3035

Table 15. [Program Management](#)

3036

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	—

3037

3038

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	—

3047

3048

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	—

3049

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

3052 **Appendix D. Change Log**

3053 This publication incorporates the following changes from the original edition (February 2020;
3054 updated January 28, 2021):

- 3055 • Streamlined introductory information in [Section 1](#) and [Section 2](#) to improve clarity and
3056 customer understanding
- 3057 • Modified the security requirements and families in [Section 3](#) to reflect the security
3058 controls in the NIST SP 800-53B [13] moderate baseline and the tailoring actions in
3059 [Appendix C](#)
- 3060 • Eliminated the distinction between basic and derived security requirements
- 3061 • Increased the specificity of security requirements to remove ambiguity, improve the
3062 effectiveness of implementation, and clarify the scope of assessments
- 3063 • Introduced organization-defined parameters (ODP) in selected security requirements to
3064 increase flexibility and help organizations better manage risk
- 3065 • Grouped security requirements, where possible, to improve understanding and efficiency
3066 of implementation and assessments
- 3067 • Removed outdated and redundant security requirements
- 3068 • Added titles to security requirements
- 3069 • Introduced a new tailoring category, *Not Applicable (NA)*
- 3070 • Recategorized selected controls in the NIST SP 800-53B moderate baseline (using the
3071 tailoring criteria in [Appendix C](#))
- 3072 • Recast the security requirements, where possible, for consistency with the security
3073 control language in NIST SP 800-53
- 3074 • Revised the structure of the [References](#), [Acronyms](#), and [Glossary](#) sections for greater
3075 clarity and ease of use
- 3076 • Revised the tailoring table in [Appendix C](#) for consistency with the changes to the security
3077 requirements

3078 [Table 23](#) shows the changes incorporated into this publication. Errata updates can include
3079 corrections, clarifications, or other minor changes in the publication that are either *editorial* or
3080 *substantive* in nature. Any potential updates to this document that are not yet published in an
3081 errata update or a formal revision, including additional issues and potential corrections, will be
3082 posted as they are identified. See the [publication details](#) for this report. The current release of this
3083 publication does not include any errata updates.

