



**NIST Special Publication
NIST SP 800-171r3 fpd**

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Final Public Draft

Ron Ross
Victoria Pillitteri

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

**NIST Special Publication
NIST SP 800-171r3 fpd**

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Final Public Draft

Ron Ross
Victoria Pillitteri
*Computer Security Division
Information Technology Laboratory*

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

November 2023



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

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

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

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

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

Authority

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

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

NIST Technical Series Policies

[Copyright, Use, and Licensing Statements](#)
[NIST Technical Series Publication Identifier Syntax](#)

How to Cite this NIST Technical Series Publication:

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

Author ORCID iDs

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

Public Comment Period

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

Submit Comments

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

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

Abstract

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

Keywords

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

Reports on Computer Systems Technology

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

Audience

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

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

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

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

Note to Reviewers

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

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

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

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

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

Call for Patent Claims

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

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

- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
- b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
 - i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
 - ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

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

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

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

Table of Contents

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	6
3.1. Access Control	6
3.1.1. Account Management	6
3.1.2. Access Enforcement	7
3.1.3. Information Flow Enforcement	8
3.1.4. Separation of Duties	8
3.1.5. Least Privilege	9
3.1.6. Least Privilege – Privileged Accounts	9
3.1.7. Least Privilege – Privileged Functions	10
3.1.8. Unsuccessful Logon Attempts	10
3.1.9. System Use Notification	11
3.1.10. Device Lock	11
3.1.11. Session Termination	12
3.1.12. Remote Access	12
3.1.13. Withdrawn	13
3.1.14. Withdrawn	13
3.1.15. Withdrawn	13
3.1.16. Wireless Access	13
3.1.17. Withdrawn	14
3.1.18. Access Control for Mobile Devices	14
3.1.19. Withdrawn	15
3.1.20. Use of External Systems	15
3.1.21. Withdrawn	16
3.1.22. Publicly Accessible Content	16
3.2. Awareness and Training	16
3.2.1. Literacy Training and Awareness	16
3.2.2. Role-Based Training	17
3.2.3. Withdrawn	18
3.3. Audit and Accountability	18

3.3.1. Event Logging	18
3.3.2. Audit Record Content	19
3.3.3. Audit Record Generation	19
3.3.4. Response to Audit Logging Process Failures	20
3.3.5. Audit Record Review, Analysis, and Reporting	20
3.3.6. Audit Record Reduction and Report Generation	21
3.3.7. Time Stamps.....	21
3.3.8. Protection of Audit Information.....	22
3.3.9. Withdrawn	22
3.4. Configuration Management	22
3.4.1. Baseline Configuration.....	22
3.4.2. Configuration Settings	23
3.4.3. Configuration Change Control	23
3.4.4. Impact Analyses	24
3.4.5. Access Restrictions for Change.....	24
3.4.6. Least Functionality	25
3.4.7. Withdrawn	25
3.4.8. Authorized Software – Allow by Exception	25
3.4.9. Withdrawn	26
3.4.10. System Component Inventory.....	26
3.4.11. Information Location	27
3.4.12. System and Component Configuration for High-Risk Areas.....	27
3.5. Identification and Authentication	28
3.5.1. User Identification, Authentication, and Re-Authentication.....	28
3.5.2. Device Identification and Authentication	28
3.5.3. Multi-Factor Authentication	29
3.5.4. Replay-Resistant Authentication.....	29
3.5.5. Identifier Management	29
3.5.6. Withdrawn	30
3.5.7. Password Management	30
3.5.8. Withdrawn	31
3.5.9. Withdrawn	31
3.5.10. Withdrawn	31
3.5.11. Authentication Feedback	31
3.5.12. Authenticator Management.....	31
3.6. Incident Response	32

3.6.1. Incident Response Plan and Handling.....	32
3.6.2. Incident Monitoring, Reporting, and Response Assistance	33
3.6.3. Incident Response Testing	33
3.6.4. Incident Response Training	34
3.7. Maintenance	34
3.7.1. Withdrawn	34
3.7.2. Withdrawn	34
3.7.3. Withdrawn	35
3.7.4. Maintenance Tools	35
3.7.5. Nonlocal Maintenance	35
3.7.6. Maintenance Personnel	36
3.8. Media Protection.....	36
3.8.1. Media Storage	36
3.8.2. Media Access	37
3.8.3. Media Sanitization	37
3.8.4. Media Marking	38
3.8.5. Media Transport.....	38
3.8.6. Withdrawn	39
3.8.7. Media Use.....	39
3.8.8. Withdrawn	39
3.8.9. System Backup – Cryptographic Protection	39
3.9. Personnel Security.....	40
3.9.1. Personnel Screening	40
3.9.2. Personnel Termination and Transfer	40
3.10. Physical Protection	41
3.10.1. Physical Access Authorizations	41
3.10.2. Monitoring Physical Access	42
3.10.3. Withdrawn	42
3.10.4. Withdrawn	42
3.10.5. Withdrawn	42
3.10.6. Alternate Work Site	42
3.10.7. Physical Access Control	43
3.10.8. Access Control for Transmission and Output Devices.....	43
3.11. Risk Assessment	44
3.11.1. Risk Assessment	44
3.11.2. Vulnerability Monitoring and Scanning.....	44

3.11.3. Withdrawn	45
3.12. Security Assessment and Monitoring	45
3.12.1. Security Assessment	45
3.12.2. Plan of Action and Milestones	46
3.12.3. Continuous Monitoring	46
3.12.4. Withdrawn	47
3.12.5. Information Exchange	47
3.13. System and Communications Protection	47
3.13.1. Boundary Protection	47
3.13.2. Withdrawn	48
3.13.3. Withdrawn	48
3.13.4. Information in Shared System Resources	48
3.13.5. Withdrawn	48
3.13.6. Network Communications – Deny by Default – Allow by Exception	49
3.13.7. Withdrawn	49
3.13.8. Transmission and Storage Confidentiality	49
3.13.9. Network Disconnect	49
3.13.10. Cryptographic Key Establishment and Management	50
3.13.11. Cryptographic Protection	50
3.13.12. Collaborative Computing Devices and Applications	51
3.13.13. Mobile Code	51
3.13.14. Withdrawn	51
3.13.15. Session Authenticity	52
3.13.16. Withdrawn	52
3.14. System and Information Integrity	52
3.14.1. Flaw Remediation	52
3.14.2. Malicious Code Protection	53
3.14.3. Security Alerts, Advisories, and Directives	53
3.14.4. Withdrawn	54
3.14.5. Withdrawn	54
3.14.6. System Monitoring	54
3.14.7. Withdrawn	55
3.14.8. Information Management and Retention	55
3.15. Planning	55
3.15.1. Policy and Procedures	55
3.15.2. System Security Plan	56

3.15.3. Rules of Behavior	57
3.16. System and Services Acquisition.....	57
3.16.1. Acquisition Process.....	57
3.16.2. Unsupported System Components	58
3.16.3. External System Services	58
3.17. Supply Chain Risk Management	59
3.17.1. Supply Chain Risk Management Plan	59
3.17.2. Acquisition Strategies, Tools, and Methods.....	60
3.17.3. Supply Chain Requirements and Processes	60
References.....	62
Appendix A. Acronyms	69
Appendix B. Glossary	71
Appendix C. Tailoring Criteria.....	79
Appendix D. Change Log.....	91

List of Tables

Table 1. Security requirement families	4
Table 2. Security control tailoring criteria	79
Table 3. Access Control (AC)	79
Table 4. Awareness and Training (AT)	80
Table 5. Audit and Accountability (AU)	80
Table 6. Assessment, Authorization, and Monitoring (CA)	81
Table 7. Configuration Management (CM)	81
Table 8. Contingency Planning (CP)	82
Table 9. Identification and Authentication (IA)	83
Table 10. Incident Response (IR)	84
Table 11. Maintenance (MA)	84
Table 12. Media Protection (MP)	84
Table 13. Physical and Environmental Protection (PE)	85
Table 14. Planning (PL)	85
Table 15. Program Management (PM)	85
Table 16. Personnel Security (PS)	86
Table 17. PII Processing and Transparency (PT)	87
Table 18. Risk Assessment (RA)	87
Table 19. System and Services Acquisition (SA)	88
Table 20. System and Communications Protection (SC)	88
Table 21. System and Information Integrity (SI)	89
Table 22. Supply Chain Risk Management (SR)	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, Eduardo Takamura, Isabel Van Wyk, and Cristina Ritfeld – for their outstanding support in preparing this document for publication. Finally, a special note of thanks goes out to Kelley Dempsey for the initial research and development of the technical content used in the prototype CUI overlay.

Historical Contributions

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

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

1. Introduction

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

The CUI regulation requires federal agencies that use federal information 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 To maintain a consistent level of protection, the security requirements for safeguarding CUI in nonfederal systems and organizations must comply with FIPS 199 [6] and FIPS 200 [7]. The requirements are derived from the controls in NIST Special Publication (SP) 800-53 [8].

1.1. Purpose and Applicability

The purpose of this publication is to provide federal agencies with recommended security requirements⁶ for protecting the *confidentiality* of CUI⁷ when such information is resident in nonfederal systems and organizations and where there are no specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI registry [4]. The requirements do not apply to nonfederal organizations that are collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency.⁸

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

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

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

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

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

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

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

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

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

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

45 **1.2. Organization of This Publication**

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

- 47 • [Section 2](#) describes the assumptions and methodology used to develop the security
48 requirements for protecting the confidentiality of CUI, the format of the requirements,
49 and the tailoring criteria applied to the NIST standards and guidelines to obtain the
50 requirements.
- 51 • [Section 3](#) lists the security requirements for protecting the confidentiality of CUI in
52 nonfederal systems and organizations.

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

- 55 • [References](#)
- 56 • [Appendix A](#): Acronyms
- 57 • [Appendix B](#): Glossary
- 58 • [Appendix C](#): Tailoring Criteria
- 59 • [Appendix D](#): Change Log

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

60 2. The Fundamentals

61 This section describes the basic assumptions and methodology used to develop the requirements
62 to protect the confidentiality of CUI in nonfederal systems and organizations. It also includes the
63 tailoring¹⁰ criteria applied to the controls in NIST SP 800-53 [8].

64 2.1. Basic Assumptions

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

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

75 2.2. Security Requirement Development Methodology

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

- 78 • Primarily the responsibility of the Federal Government;
- 79 • Not directly related to protecting the confidentiality of CUI;
- 80 • Adequately addressed by other related controls;¹² or
- 81 • Not applicable.

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

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

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

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

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

87

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

88

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

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

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

106 **3.13.11 Cryptographic Protection**

107 **REQUIREMENT:** 03.13.11

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

110 **DISCUSSION**

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

113 **REFERENCES**

114 Source Control: [SC-13](#)
115 Supporting Publications: FIPS 140-3 [38]

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

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

ORGANIZATION-DEFINED PARAMETERS

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

116

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

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

125 **3. The Requirements**

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

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

139 **3.1. [Access Control](#)**

140 **3.1.1. Account Management**

141 **REQUIREMENT:** 03.01.01

- 142 a. Define the types of system accounts allowed and prohibited.
- 143 b. Create, enable, modify, disable, and remove system accounts in accordance with
144 organizational policy, procedures, prerequisites, and criteria.
- 145 c. Specify authorized users of the system, group and role membership, and access
146 authorizations (i.e., privileges).
- 147 d. Authorize access to the system based on a valid access authorization and intended system
148 usage.
- 149 e. Monitor the use of system accounts.
- 150 f. Disable system accounts when:
- 151 1. The accounts have expired;
- 152 2. The accounts have been inactive for [*Assignment: organization-defined time period*];
- 153 3. The accounts are no longer associated with a user or individual;
- 154 4. The accounts are in violation of organizational policy; or
- 155 5. Significant risks associated with individuals are discovered.
- 156 g. Notify organizational personnel or roles when:
- 157 1. Accounts are no longer required;
- 158 2. Users are terminated or transferred; and
- 159 3. System usage or need-to-know changes for an individual.

160 **DISCUSSION**

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

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

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

181 **REFERENCES**

182 Source Controls: [AC-02](#), [AC-02\(03\)](#), [AC-02\(13\)](#)
183 Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17],
184 SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-
185 178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

186 **3.1.2. Access Enforcement**

187 **REQUIREMENT:** 03.01.02

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

189 **DISCUSSION**

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

197 **REFERENCES**

198 Source Control: [AC-03](#)
199 Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17],
200 SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-
201 178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

202 3.1.3. Information Flow Enforcement

203 **REQUIREMENT:** 03.01.03

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

206 **DISCUSSION**

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

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

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

232 **REFERENCES**

233 Source Control: [AC-04](#)

234 Supporting Publications: SP 800-160-1 [11], SP 800-162 [22], SP 800-178 [23]

235 3.1.4. Separation of Duties

236 **REQUIREMENT:** 03.01.04

237 a. Identify the duties of individuals requiring separation.

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

239 **DISCUSSION**

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

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

249 REFERENCES

250 Source Control: [AC-05](#)
251 Supporting Publications: SP 800-162 [22], SP 800-178 [23]

252 3.1.5. Least Privilege

253 REQUIREMENT: 03.01.05

- 254 a. Allow only authorized system access for users (or processes acting on behalf of users) that is
255 necessary to accomplish assigned organizational tasks.
- 256 b. Authorize access to [*Assignment: organization-defined security functions and security-*
257 *relevant information*].
- 258 c. Review the privileges assigned to roles or classes of users periodically to validate the need
259 for such privileges.
- 260 d. Reassign or remove privileges, as necessary.

261 DISCUSSION

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

271 REFERENCES

272 Source Controls: [AC-06](#), [AC-06\(01\)](#), [AC-06\(07\)](#), [AU-09\(04\)](#)
273 Supporting Publications: None

274 3.1.6. Least Privilege – Privileged Accounts

275 REQUIREMENT: 03.01.06

- 276 a. Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or*
277 *roles*].
- 278 b. Require that users (or roles) with privileged accounts use non-privileged accounts when
279 accessing nonsecurity functions or nonsecurity information.

280 **DISCUSSION**

281 Privileged accounts are typically described as system administrator accounts. Restricting
282 privileged accounts to specific personnel or roles prevents nonprivileged users from accessing
283 security functions or security-relevant information. Requiring the use of non-privileged accounts
284 when accessing nonsecurity functions or nonsecurity information limits exposure when operating
285 from within privileged accounts. Including roles addresses situations in which organizations
286 implement access control policies, such as role-based access control, and where a change of role
287 provides the same degree of assurance in the change of access authorizations for the user and the
288 processes acting on behalf of the user as would be provided by a change between a privileged and
289 non-privileged account.

290 **REFERENCES**

291 Source Controls: [AC-06\(02\)](#), [AC-06\(05\)](#)
292 Supporting Publications: None

293 **3.1.7. Least Privilege – Privileged Functions**

294 **REQUIREMENT:** 03.01.07

- 295 a. Prevent non-privileged users from executing privileged functions.
296 b. Log the execution of privileged functions.

297 **DISCUSSION**

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

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

310 **REFERENCES**

311 Source Controls: [AC-06\(09\)](#), [AC-06\(10\)](#)
312 Supporting Publications: None

313 **3.1.8. Unsuccessful Logon Attempts**

314 **REQUIREMENT:** 03.01.08

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

317 **DISCUSSION**

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

323 **REFERENCES**

324 Source Control: [AC-07](#)
325 Supporting Publications: SP 800-63-3 [27], SP 800-124 [28]

326 **3.1.9. System Use Notification**

327 **REQUIREMENT:** 03.01.09

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

330 **DISCUSSION**

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

337 **REFERENCES**

338 Source Control: [AC-08](#)
339 Supporting Publications: None

340 **3.1.10. Device Lock**

341 **REQUIREMENT:** 03.01.10

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

349 **DISCUSSION**

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

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

359 **REFERENCES**

360 Source Controls: [AC-11](#), [AC-11\(01\)](#)
361 Supporting Publications: None

362 **3.1.11. Session Termination**

363 **REQUIREMENT:** 03.01.11

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

366 **DISCUSSION**

367 This requirement addresses the termination of user-initiated logical sessions in contrast to the
368 termination of network connections that are associated with communications sessions (i.e.,
369 disconnecting from the network) in [03.13.09](#). A logical session is initiated whenever a user (or
370 processes acting on behalf of a user) accesses a system. Logical sessions can be terminated (and
371 thus terminate user access) without terminating network sessions. Session termination ends all
372 system processes associated with a user's logical session except those processes that are created
373 by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger
374 events that require automatic session termination can include organization-defined periods of
375 user inactivity, time-of-day restrictions on system use, and targeted responses to certain types of
376 incidents.

377 **REFERENCES**

378 Source Control: [AC-12](#)
379 Supporting Publications: None

380 **3.1.12. Remote Access**

381 **REQUIREMENT:** 03.01.12

- 382 a. Establish usage restrictions, configuration requirements, and connection requirements for
383 each type of allowable remote system access.
- 384 b. Authorize each type of remote system access prior to establishing such connections.
- 385 c. Route remote access to the system through authorized and managed access control points.
- 386 d. Authorize remote execution of privileged commands and remote access to security-relevant
387 information.

388 **DISCUSSION**

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

395 Restricting the execution of privileged commands and access to security-relevant information
396 via remote access reduces the exposure of the organization and its susceptibility to threats by
397 adversaries. A privileged command is a human-initiated command executed on a system that
398 involves the control, monitoring, or administration of the system, including security functions
399 and security-relevant information. Security-relevant information is information that can
400 potentially impact the operation of security functions or the provision of security services in a
401 manner that could result in failure to enforce the system security policy or maintain isolation of
402 code and data. Privileged commands give individuals the ability to execute sensitive, security-
403 critical, or security-relevant system functions. Controlling access from remote locations helps to
404 ensure that unauthorized individuals are unable to execute such commands with the potential to
405 do serious or catastrophic damage to the system.

406 REFERENCES

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

410 3.1.13. Withdrawn

411 Incorporated into [03.01.12](#).

412 3.1.14. Withdrawn

413 Incorporated into [03.01.12](#).

414 3.1.15. Withdrawn

415 Incorporated into [03.01.12](#).

416 3.1.16. Wireless Access

417 REQUIREMENT: 03.01.16

- 418 a. Establish usage restrictions, configuration requirements, and connection requirements for
419 each type of wireless access to the system.
- 420 b. Authorize each type of wireless access to the system prior to establishing such
421 connections.
- 422 c. Disable, when not intended for use, wireless networking capabilities prior to issuance and
423 deployment.

424 DISCUSSION

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

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

436 REFERENCES

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

439 3.1.17. Withdrawn

440 Incorporated into [03.01.16](#).

441 3.1.18. Access Control for Mobile Devices

442 **REQUIREMENT:** 03.01.18

- 443 a. Establish usage restrictions, configuration requirements, and connection requirements for
444 mobile devices.
- 445 b. Authorize the connection of mobile devices to the system.
- 446 c. Implement full-device or container-based encryption to protect the confidentiality of CUI on
447 mobile devices.

448 DISCUSSION

449 A mobile device is a computing device that has a small form factor such that it can easily be
450 carried by a single individual; is designed to operate without a physical connection; possesses
451 local, non-removable, or removable data storage; and includes a self-contained power source.
452 Mobile device functionality may also include voice communication capabilities, on-board
453 sensors that allow the device to capture information, and/or built-in features for synchronizing
454 local data with remote locations. Examples include smart phones, smart watches, and tablets.
455 Mobile devices are typically associated with a single individual. The processing, storage, and
456 transmission capability of mobile devices may be comparable to or a subset of notebook or
457 desktop systems, depending on the nature and intended purpose of the device. The protection
458 and control of mobile devices is behavior- or policy-based and requires users to take physical
459 action to protect and control such devices when outside of controlled areas. Controlled areas are
460 spaces for which the organization provides physical or procedural controls to meet the
461 requirements established for protecting CUI.

462 Due to the large variety of mobile devices with different characteristics and capabilities,
463 organizational restrictions may vary for the different classes or types of such devices. Usage
464 restrictions, configuration requirements, and connection requirements for mobile devices
465 include configuration management, device identification and authentication, implementing
466 mandatory protective software, scanning devices for malicious code, updating virus protection
467 software, scanning for critical software updates and patches, conducting primary operating
468 system (and possibly other resident software) integrity checks, and disabling unnecessary
469 hardware. Organizations can employ full-device encryption or container-based encryption to
470 protect the confidentiality of CUI on mobile devices. Container-based encryption provides a
471 fine-grained approach to the encryption of data and information, including encrypting selected
472 data structures (e.g., files, records, or fields).

473 **REFERENCES**

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

476 **3.1.19. Withdrawn**

477 Incorporated into [03.01.18](#).

478 **3.1.20. Use of External Systems**

479 **REQUIREMENT: 03.01.20**

- 480 a. Prohibit the use of external systems unless the systems are specifically authorized.
- 481 b. Establish the following terms, conditions, and security requirements to be satisfied on
482 external systems prior to allowing use of or access to those systems by authorized
483 individuals: [*Assignment: organization-defined terms, conditions, and requirements*].
- 484 c. Permit authorized individuals to use an external system to access the organizational system
485 or to process, store, or transmit CUI only after:
- 486 1. Verification of the implementation of security requirements on the external system as
487 specified in the organization's security plans; and
- 488 2. Retention of approved system connection or processing agreements with the
489 organizational entity hosting the external system.
- 490 d. Restrict the use of organization-controlled portable storage devices by authorized
491 individuals on external systems.

492 **DISCUSSION**

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

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

508 **REFERENCES**

509 Source Controls: [AC-20](#), [AC-20\(01\)](#), [AC-20\(02\)](#)
510 Supporting Publications: None

511 **3.1.21. Withdrawn**

512 Incorporated into [03.01.20](#).

513 **3.1.22. Publicly Accessible Content**

514 **REQUIREMENT:** 03.01.22

- 515 a. Train authorized individuals to ensure that publicly accessible information does not contain
516 CUI.
- 517 b. Review the content on publicly accessible systems for CUI periodically and remove such
518 information, if discovered.

519 **DISCUSSION**

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

523 **REFERENCES**

524 Source Control: [AC-22](#)
525 Supporting Publications: None

526 **3.2. [Awareness and Training](#)**

527 **3.2.1. Literacy Training and Awareness**

528 **REQUIREMENT:** 03.02.01

- 529 a. Provide security literacy training to system users:
- 530 1. As part of initial training for new users and periodically thereafter;
- 531 2. When required by system changes or following [*Assignment: organization-defined*
532 *events*]; and
- 533 3. On recognizing and reporting indicators of insider threat, social engineering, and social
534 mining.
- 535 b. Update security literacy training content periodically and following [*Assignment: organization-*
536 *defined events*].

537 **DISCUSSION**

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

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

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

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

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

569 REFERENCES

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

572 3.2.2. Role-Based Training

573 REQUIREMENT: 03.02.02

- 574 a. Provide role-based security training to organizational personnel:
- 575 1. Before authorizing access to the system or CUI, before performing assigned duties, and
576 periodically thereafter; and
 - 577 2. When required by system changes or following [*Assignment: organization-defined*
578 *events*].
- 579 b. Update role-based training content periodically and following [*Assignment: organization-*
580 *defined events*].

581 DISCUSSION

582 Organizations determine the content and frequency of security training based on the assigned
583 duties, roles, and responsibilities of individuals and the security requirements of the systems to
584 which personnel have authorized access. In addition, organizations provide system developers,
585 enterprise architects, security architects, software developers, systems integrators,
586 acquisition/procurement officials, system and network administrators, personnel conducting
587 configuration management and auditing activities, personnel performing independent verification
588 and validation, security assessors, and personnel with access to system-level software with
589 security-related technical training specifically tailored for their assigned duties.

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

595 REFERENCES

596 Source Control: [AT-03](#)
597 Supporting Publications: SP 800-161 [33], SP 800-181 [34]

598 3.2.3. Withdrawn

599 Incorporated into [03.02.01](#).

600 3.3. [Audit and Accountability](#)

601 3.3.1. Event Logging

602 **REQUIREMENT:** 03.03.01

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

606 DISCUSSION

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

624 REFERENCES

625 Source Control: [AU-02](#)
626 Supporting Publications: SP 800-92 [35]

627 **3.3.2. Audit Record Content**

628 **REQUIREMENT:** 03.03.02

- 629 a. Include the following content in audit records:
- 630 1. What type of event occurred;
 - 631 2. When the event occurred;
 - 632 3. Where the event occurred;
 - 633 4. Source of the event;
 - 634 5. Outcome of the event; and
 - 635 6. Identity of individuals, subjects, objects, or entities associated with the event.
- 636 b. Provide additional information for audit records, as needed.

637 **DISCUSSION**

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

644 **REFERENCES**

645 Source Controls: [AU-03](#), [AU-03\(01\)](#)
646 Supporting Publications: None

647 **3.3.3. Audit Record Generation**

648 **REQUIREMENT:** 03.03.03

- 649 a. Generate audit records for the selected event types and audit record content specified in
650 [03.03.01](#) and [03.03.02](#).
- 651 b. Retain audit records for a time period consistent with records retention policy.

652 **DISCUSSION**

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

661 **REFERENCES**

662 Source Controls: [AU-11](#), [AU-12](#)
663 Supporting Publications: SP 800-92 [35]

664 3.3.4. Response to Audit Logging Process Failures

665 **REQUIREMENT:** 03.03.04

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

669 **DISCUSSION**

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

681 **REFERENCES**

682 Source Control: [AU-05](#)
683 Supporting Publications: None

684 3.3.5. Audit Record Review, Analysis, and Reporting

685 **REQUIREMENT:** 03.03.05

- 686 a. Review and analyze system audit records periodically for indications and potential impact of
687 inappropriate or unusual activity.
- 688 b. Report findings to organizational personnel or roles.
- 689 c. Analyze and correlate audit records across different repositories to gain organization-wide
690 situational awareness.

691 **DISCUSSION**

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

706 **REFERENCES**

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

709 **3.3.6. Audit Record Reduction and Report Generation**

710 **REQUIREMENT: 03.03.06**

- 711 a. Implement an audit record reduction and report generation capability that supports audit
712 record review, analysis, reporting requirements, and after-the-fact investigations of incidents.
713 b. Preserve the original content and time ordering of audit records.

714 **DISCUSSION**

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

724 **REFERENCES**

725 Source Control: [AU-07](#)
726 Supporting Publications: None

727 **3.3.7. Time Stamps**

728 **REQUIREMENT: 03.03.07**

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

735 **DISCUSSION**

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

744 **REFERENCES**

745 Source Control: [AU-08](#)
746 Supporting Publications: None

747 **3.3.8. Protection of Audit Information**

748 **REQUIREMENT:** 03.03.08

- 749 a. Protect audit information and audit logging tools from unauthorized access, modification, and
750 deletion.
- 751 b. Authorize access to management of audit logging functionality to only a subset of privileged
752 users or roles.

753 **DISCUSSION**

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

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

764 **REFERENCES**

765 Source Controls: [AU-09](#), [AU-09\(04\)](#)
766 Supporting Publications: None

767 **3.3.9. Withdrawn**

768 Incorporated into [03.03.08](#).

769 **3.4. [Configuration Management](#)**

770 **3.4.1. Baseline Configuration**

771 **REQUIREMENT:** 03.04.01

- 772 a. Develop and maintain under configuration control, a current baseline configuration of the
773 system.
- 774 b. Review and update the baseline configuration of the system periodically and when system
775 components are installed or modified.

776 **DISCUSSION**

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

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

785 REFERENCES

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

788 3.4.2. Configuration Settings

789 REQUIREMENT: 03.04.02

- 790 a. Establish, document, and implement the following configuration settings for the system that
791 reflect the most restrictive mode consistent with operational requirements: [*Assignment:*
792 *organization-defined configuration settings*].
- 793 b. Identify, document, and approve any deviations from established configuration settings.

794 DISCUSSION

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

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

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

815 REFERENCES

816 Source Control: [CM-06](#)
817 Supporting Publications: SP 800-70 [44], SP 800-126 [45], SP 800-128 [41]

818 3.4.3. Configuration Change Control

819 REQUIREMENT: 03.04.03

- 820 a. Define the types of changes to the system that are configuration-controlled.
- 821 b. Review proposed configuration-controlled changes to the system and approve or disapprove
- 822 such changes with explicit consideration for security impacts.
- 823 c. Implement and document approved configuration-controlled changes to the system.
- 824 d. Monitor and review activities associated with configuration-controlled changes to the system.

825 **DISCUSSION**

826 Configuration change control refers to tracking, reviewing, approving or disapproving, and

827 logging changes to the system. Specifically, it involves the systematic proposal, justification,

828 implementation, testing, review, and disposition of changes to the system, including system

829 upgrades and modifications. Configuration change control includes changes to baseline

830 configurations for system components (e.g., operating systems, applications, firewalls, routers,

831 mobile devices) and configuration items of the system, changes to configuration settings,

832 unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

833 **REFERENCES**

834 Source Control: [CM-03](#)

835 Supporting Publications: SP 800-124 [28], SP 800-128 [41]

836 **3.4.4. Impact Analyses**

837 **REQUIREMENT:** 03.04.04

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

839 **DISCUSSION**

840 Organizational personnel with security responsibilities conduct impact analyses that include

841 reviewing security plans, policies, and procedures to understand security requirements; reviewing

842 system design documentation and operational procedures to understand how system changes

843 might affect the security state of the system; reviewing the impacts of changes on supply chain

844 partners with stakeholders; and determining how potential changes to a system create new risks

845 and the ability to mitigate those risks. Impact analyses also include risk assessments to understand

846 the impacts of changes and to determine whether additional security requirements are needed.

847 **REFERENCES**

848 Source Control: [CM-04](#)

849 Supporting Publications: SP 800-128 [41]

850 **3.4.5. Access Restrictions for Change**

851 **REQUIREMENT:** 03.04.05

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

853 changes to the system.

854 **DISCUSSION**

855 Changes to the hardware, software, or firmware components of the system or the operational

856 procedures related to the system can have potentially significant effects on the security of the

857 system. Therefore, organizations permit only qualified and authorized individuals to access the

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

862 REFERENCES

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

865 3.4.6. Least Functionality

866 REQUIREMENT: 03.04.06

- 867 a. Configure the system to provide only mission-essential capabilities.
- 868 b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services:
869 [*Assignment: organization-defined functions, ports, protocols, connections, and services*].
- 870 c. Review the system periodically to identify unnecessary or nonsecure functions, ports,
871 protocols, connections, and services.
- 872 d. Disable or remove functions, ports, protocols, connections, and services that are
873 unnecessary or nonsecure.

874 DISCUSSION

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

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

889 REFERENCES

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

892 3.4.7. Withdrawn

893 Incorporated into [03.04.06](#).

894 3.4.8. Authorized Software – Allow by Exception

895 REQUIREMENT: 03.04.08

- 896 a. Identify software programs authorized to execute on the system.
- 897 b. Implement a deny-all, allow-by-exception policy for the execution of software programs on the
- 898 system.
- 899 c. Review and update the list of authorized software programs periodically.

900 **DISCUSSION**

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

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

919 **REFERENCES**

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

922 **3.4.9. Withdrawn**

923 Addressed by [03.01.05](#), [03.01.06](#), [03.01.07](#), and [03.04.08](#).

924 **3.4.10. System Component Inventory**

925 **REQUIREMENT:** 03.04.10

- 926 a. Develop and document an inventory of system components.
- 927 b. Review and update the system component inventory periodically.
- 928 c. Update the system component inventory as part of installations, removals, and system
- 929 updates.

930 **DISCUSSION**

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

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

941 **REFERENCES**

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

944 **3.4.11. Information Location**

945 **REQUIREMENT:** 03.04.11

- 946 a. Identify and document the location of CUI and the system components on which the
947 information is processed and stored.
- 948 b. Identify and document the users who have access to the system and system components
949 where CUI is processed and stored.
- 950 c. Document changes to the location (i.e., system or system components) where CUI is
951 processed and stored.

952 **DISCUSSION**

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

957 **REFERENCES**

958 Source Control: [CM-12](#)
959 Supporting Publications: None

960 **3.4.12. System and Component Configuration for High-Risk Areas**

961 **REQUIREMENT:** 03.04.12

- 962 a. Issue systems or system components with the following configurations to individuals
963 traveling to high-risk locations: [*Assignment: organization-defined system configurations*].
- 964 b. Apply the following security requirements to the system or system components when the
965 individuals return from travel: [*Assignment: organization-defined security requirements*].

966 **DISCUSSION**

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

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

977 **REFERENCES**

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

980 **3.5. [Identification and Authentication](#)**

981 **3.5.1. User Identification, Authentication, and Re-Authentication**

982 **REQUIREMENT:** 03.05.01

- 983 a. Uniquely identify and authenticate system users and associate that unique identification with
984 processes acting on behalf of those users.
- 985 b. Re-authenticate users when [*Assignment: organization-defined circumstances or situations*
986 *requiring re-authentication*].

987 **DISCUSSION**

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

998 **REFERENCES**

999 Source Controls: [IA-02](#), [IA-11](#)
1000 Supporting Publications: SP 800-63-3 [27]

1001 **3.5.2. Device Identification and Authentication**

1002 **REQUIREMENT:** 03.05.02

1003 Uniquely identify and authenticate devices before establishing a system connection.

1004 **DISCUSSION**

1005 Devices that require unique device-to-device identification and authentication are defined by
1006 type, device, or a combination of type and device. Organization-defined device types include
1007 devices that are not owned by the organization. Systems use shared known information (e.g.,
1008 Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP]
1009 addresses) for device identification or organizational authentication solutions (e.g., Institute of
1010 Electrical and Electronics Engineers [IEEE] 802.1x and Extensible Authentication Protocol
1011 [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to

1012 identify and authenticate devices on local and wide area networks. PKI and certificate revocation
1013 checking for the certificates exchanged can also be included as part of device authentication.

1014 **REFERENCES**

1015 Source Control: [IA-03](#)
1016 Supporting Publications: SP 800-63-3 [27]

1017 **3.5.3. Multi-Factor Authentication**

1018 **REQUIREMENT:** 03.05.03

1019 Implement multi-factor authentication for access to system accounts.

1020 **DISCUSSION**

1021 Multi-factor authentication requires the use of two or more different factors to achieve
1022 authentication. The authentication factors are defined as follows: something you know (e.g., a
1023 personal identification number [PIN]), something you have (e.g., a physical authenticator, such as
1024 a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication
1025 solutions that feature physical authenticators include hardware authenticators that provide time-
1026 based or challenge-response outputs and smart cards. In addition to authenticating users at the
1027 system level, organizations may also employ authentication mechanisms at the application level
1028 to provide increased information security.

1029 **REFERENCES**

1030 Source Controls: [IA-02\(01\)](#), [IA-02\(02\)](#)
1031 Supporting Publications: SP 800-63-3 [27]

1032 **3.5.4. Replay-Resistant Authentication**

1033 **REQUIREMENT:** 03.05.04

1034 Implement replay-resistant authentication mechanisms for access to system accounts.

1035 **DISCUSSION**

1036 Authentication processes resist replay attacks if it is impractical to successfully authenticate by
1037 recording or replaying previous authentication messages. Replay-resistant techniques include
1038 protocols that use nonces or challenges, such as time synchronous or challenge-response one-time
1039 authenticators.

1040 **REFERENCES**

1041 Source Control: [IA-02\(08\)](#)
1042 Supporting Publications: SP 800-63-3 [27]

1043 **3.5.5. Identifier Management**

1044 **REQUIREMENT:** 03.05.05

1045 a. Receive authorization from organizational personnel or roles to assign an individual, group,
1046 role, service, or device identifier.

- 1047 b. Select and assign an identifier that identifies an individual, group, role, service, or device.
- 1048 c. Prevent reuse of identifiers for [*Assignment: organization-defined time period*].
- 1049 d. Uniquely identify the status of each individual with an identifying characteristic.

1050 **DISCUSSION**

1051 Identifiers are provided for users, processes acting on behalf of users, and devices. Prohibiting the
1052 reuse of identifiers prevents the assignment of previously used individual, group, role, service, or
1053 device identifiers to different individuals, groups, roles, services, or devices. Characteristics that
1054 identify the status of individuals include contractors, foreign nationals, and non-organizational
1055 users. Identifying the status of individuals by these characteristics provides useful information
1056 about the people with whom organizational personnel are communicating. For example, is useful
1057 for an employee to know that one of the individuals on an email message is a contractor.

1058 **REFERENCES**

1059 Source Controls: [IA-04](#), [IA-04\(04\)](#)
1060 Supporting Publications: SP 800-63-3 [27]

1061 **3.5.6. Withdrawn**

1062 **3.5.7. Password Management**

1063 **REQUIREMENT: 03.05.07**

- 1064 a. Maintain a list of commonly-used, expected, or compromised passwords and update the list
1065 periodically and when organizational passwords are suspected to have been compromised.
- 1066 b. Verify, when users create or update passwords, that the passwords are not found on the list
1067 of commonly-used, expected, or compromised passwords.
- 1068 c. Transmit passwords only over cryptographically-protected channels.
- 1069 d. Store passwords in a cryptographically-protected form.
- 1070 e. Select a new password upon first use after account recovery.
- 1071 f. Enforce the following composition and complexity rules for passwords: [*Assignment:*
1072 *organization-defined composition and complexity rules*].

1073 **DISCUSSION**

1074 Password-based authentication applies to passwords used in single-factor or multi-factor
1075 authentication. Long passwords or passphrases are preferable to shorter passwords. Enforced
1076 composition rules provide marginal security benefits while decreasing usability. However,
1077 organizations may choose to establish certain rules for password generation (e.g., minimum
1078 character length) under certain circumstances and can enforce this requirement. For example,
1079 account recovery can occur when a password is forgotten. Cryptographically protected passwords
1080 include salted one-way cryptographic hashes of passwords. The list of commonly used,
1081 compromised, or expected passwords includes passwords obtained from previous breach
1082 corpuses, dictionary words, and repetitive or sequential characters. The list includes context-
1083 specific words, such as the name of the service, username, and derivatives thereof. Changing
1084 temporary passwords to permanent passwords immediately after system logon ensures that the
1085 necessary strength of the authentication mechanism is implemented at the earliest opportunity and

1086 reduces the susceptibility to authenticator compromises. Long passwords and passphrases can be
1087 used to increase the complexity of passwords.

1088 **REFERENCES**

1089 Source Control: [IA-05\(01\)](#)
1090 Supporting Publications: SP 800-63-3 [27]

1091 **3.5.8. Withdrawn**

1092 **3.5.9. Withdrawn**

1093 Incorporated into [03.05.07](#).

1094 **3.5.10. Withdrawn**

1095 Incorporated into [03.05.07](#).

1096 **3.5.11. Authentication Feedback**

1097 **REQUIREMENT:** 03.05.11

1098 Obscure feedback of authentication information during the authentication process.

1099 **DISCUSSION**

1100 The feedback from systems does not provide information that would allow unauthorized
1101 individuals to compromise authentication mechanisms. For example, for desktop or notebook
1102 computers with relatively large monitors, the threat may be significant (often referred to as
1103 shoulder surfing). For mobile devices with small displays, this threat may be less significant and
1104 is balanced against the increased likelihood of input errors due to small keyboards. Therefore,
1105 the means for obscuring the authenticator feedback is selected accordingly. Obscuring feedback
1106 includes displaying asterisks when users type passwords into input devices or displaying
1107 feedback for a limited time before fully obscuring it.

1108 **REFERENCES**

1109 Source Control: [IA-06](#)
1110 Supporting Publications: None

1111 **3.5.12. Authenticator Management**

1112 **REQUIREMENT:** 03.05.12

- 1113 a. Verify the identity of the individual, group, role, service, or device receiving the authenticator
1114 as part of the initial authenticator distribution.
- 1115 b. Establish initial authenticator content for any authenticators issued by the organization.
- 1116 c. Establish and implement administrative procedures for initial authenticator distribution, for
1117 lost, compromised, or damaged authenticators, and for revoking authenticators.
- 1118 d. Change default authenticators at first use.

- 1119 e. Change or refresh authenticators periodically or when the following events occur:
- 1120 *[Assignment: organization-defined events].*
- 1121 f. Protect authenticator content from unauthorized disclosure and modification.

1122 **DISCUSSION**

1123 Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time
1124 password devices, and ID badges. The initial authenticator content is the actual content of the
1125 authenticator (e.g., the initial password). In contrast, requirements for authenticator content
1126 contain specific characteristics. Authenticator management is supported by organization-defined
1127 settings and restrictions for various authenticator characteristics (e.g., password complexity and
1128 composition rules, validation time window for time synchronous one-time tokens, and the
1129 number of allowed rejections during the verification stage of biometric authentication).

1130 The requirement to protect individual authenticators may be implemented by [03.15.03](#) for
1131 authenticators in the possession of individuals and by [03.01.01](#), [03.01.02](#), [03.01.05](#), and
1132 [03.13.08](#) for authenticators stored in organizational systems. This includes passwords stored in
1133 hashed or encrypted formats or files that contain encrypted or hashed passwords accessible with
1134 administrator privileges. Actions can be taken to protect authenticators, including maintaining
1135 possession of authenticators, not sharing authenticators with others, and immediately reporting
1136 lost, stolen, or compromised authenticators. Developers may deliver system components with
1137 factory default authentication credentials to allow for initial installation and configuration.
1138 Default authentication credentials are often well-known, easily discoverable, and present a
1139 significant risk. Authenticator management includes issuing and revoking authenticators for
1140 temporary access when no longer needed. The use of long passwords or passphrases may
1141 obviate the need to periodically change authenticators.

1142 **REFERENCES**

- 1143 Source Control: [IA-05](#)
- 1144 Supporting Publications: SP 800-63-3 [27]

1145 **3.6. [Incident Response](#)**

1146 **3.6.1. Incident Response Plan and Handling**

1147 **REQUIREMENT:** 03.06.01

- 1148 a. Develop an incident response plan that provides the organization with a roadmap for
1149 implementing its incident response capability.
- 1150 b. Implement an incident-handling capability for incidents that is consistent with the incident
1151 response plan and includes preparation, detection and analysis, containment, eradication,
1152 and recovery.
- 1153 c. Update the incident response plan to address system and organizational changes or
1154 problems encountered during plan implementation, execution, or testing.

1155 **DISCUSSION**

1156 It is important that organizations develop and implement a coordinated approach to incident
1157 response. Organizational mission and business functions determine the structure of incident
1158 response capabilities. Incident-related information can be obtained from a variety of sources,
1159 including audit monitoring, network monitoring, physical access monitoring, user and

1160 administrator reports, and reported supply chain events. An effective incident handling capability
1161 involves coordination among many organizational entities, including mission and business
1162 owners, system owners, human resources offices, physical and personnel security offices, legal
1163 departments, operations personnel, and procurement offices.

1164 REFERENCES

1165 Source Controls: [IR-04](#), [IR-08](#)
1166 Supporting Publications: SP 800-50 [32], SP 800-61 [47], SP 800-161 [33]

1167 3.6.2. Incident Monitoring, Reporting, and Response Assistance

1168 REQUIREMENT: 03.06.02

- 1169 a. Track and document system security incidents.
- 1170 b. Report suspected incidents to the organizational incident response capability within
1171 [*Assignment: organization-defined time period*].
- 1172 c. Report incident information to [*Assignment: organization-defined authorities*].
- 1173 d. Provide an incident response support resource that offers advice and assistance to users of
1174 the system for the handling and reporting of incidents.

1175 DISCUSSION

1176 Documenting incidents includes maintaining records about each incident, the status of the
1177 incident, and other pertinent information necessary for forensics as well as evaluating incident
1178 details, trends, and handling. Incident information can be obtained from many sources, including
1179 network monitoring, incident reports, incident response teams, user complaints, supply chain
1180 partners, audit monitoring, physical access monitoring, and user and administrator reports. 3.6.1
1181 provides information on the types of incidents that are appropriate for monitoring. The types of
1182 incidents reported, the content and timeliness of the reports, and the reporting authorities reflect
1183 applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.
1184 Incident information informs risk assessments, the effectiveness of security assessments, the
1185 security requirements for acquisitions, and the selection criteria for technology products. Incident
1186 response support resources provided by organizations include help desks, assistance groups,
1187 automated ticketing systems to open and track incident response tickets, and access to forensic
1188 services or consumer redress services, when required.

1189 REFERENCES

1190 Source Controls: [IR-05](#), [IR-06](#), [IR-07](#)
1191 Supporting Publications: SP 800-61 [47], SP 800-86 [36]

1192 3.6.3. Incident Response Testing

1193 REQUIREMENT: 03.06.03

1194 Test the effectiveness of the incident response capability periodically.

1195 DISCUSSION

1196 Organizations test incident response capabilities to determine their effectiveness and identify
1197 potential weaknesses or deficiencies. Incident response testing includes the use of checklists,
1198 walk-through or tabletop exercises, and simulations. Incident response testing can include a

1199 determination of the effects of incident response on organizational operations, organizational
1200 assets, and individuals. Qualitative and quantitative data can help determine the effectiveness of
1201 incident response processes.

1202 REFERENCES

1203 Source Control: [IR-03](#)
1204 Supporting Publications: SP 800-84 [48]

1205 3.6.4. Incident Response Training

1206 REQUIREMENT: 03.06.04

- 1207 a. Provide incident response training to system users consistent with assigned roles and
1208 responsibilities:
- 1209 1. Within [*Assignment: organization-defined time period*] of assuming an incident response
1210 role or responsibility or acquiring system access;
 - 1211 2. When required by system changes; and
 - 1212 3. Periodically thereafter.
- 1213 b. Review and update incident response training content periodically and following [*Assignment:*
1214 *organization-defined events*].

1215 DISCUSSION

1216 Incident response training is associated with the assigned roles and responsibilities of
1217 organizational personnel to ensure that the appropriate content and level of detail are included in
1218 such training. For example, users may only need to know whom to call or how to recognize an
1219 incident; system administrators may require additional training on how to handle incidents; and
1220 incident responders may receive specific training on forensics, data collection techniques,
1221 reporting, system recovery, and system restoration. Incident response training includes user
1222 training in identifying and reporting suspicious activities from external and internal sources.
1223 Incident response training for users may be provided as part of [03.02.02](#). Events that may
1224 precipitate an update to incident response training content include incident response plan testing,
1225 response to an actual incident, audit or assessment findings, or changes in applicable laws,
1226 Executive Orders, policies, directives, regulations, standards, and guidelines.

1227 REFERENCES

1228 Source Control: [IR-02](#)
1229 Supporting Publications: SP 800-86 [36], SP 800-137 [49]

1230 3.7. [Maintenance](#)

1231 3.7.1. Withdrawn

1232 Recategorized as NCO.

1233 3.7.2. Withdrawn

1234 Incorporated into [03.07.04](#) and [03.07.06](#).

1235 **3.7.3. Withdrawn**

1236 Incorporated into [03.08.03](#).

1237 **3.7.4. Maintenance Tools**

1238 **REQUIREMENT:** 03.07.04

- 1239 a. Approve, control, and monitor the use of system maintenance tools.
- 1240 b. Inspect the maintenance tools for improper or unauthorized modifications.
- 1241 c. Check media containing diagnostic and test programs for malicious code before the media
1242 are used in the system.
- 1243 d. Prevent the removal of system maintenance equipment containing CUI by:
- 1244 1. Verifying that there is no CUI on the equipment;
- 1245 2. Sanitizing or destroying the equipment; or
- 1246 3. Retaining the equipment within the facility.

1247 **DISCUSSION**

1248 Approving, controlling, monitoring, and reviewing maintenance tools address security-related
1249 issues associated with the tools that are used for diagnostic and repair actions on the system.
1250 Maintenance tools can include hardware and software diagnostic and test equipment as well as
1251 packet sniffers. The tools may be pre-installed, brought in with maintenance personnel on media,
1252 cloud-based, or downloaded from a website. Diagnostic and test programs are potential vehicles
1253 for transporting malicious code into the system, either intentionally or unintentionally. Examples
1254 of media inspection include checking the cryptographic hash or digital signatures of diagnostic
1255 and test programs and/or media. If organizations inspect media that contain diagnostic and test
1256 programs and determine that the media also contains malicious code, the incident is handled
1257 consistent with incident handling policies and procedures. A periodic review of maintenance tools
1258 can result in the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used
1259 tools. Maintenance tools do not address the hardware and software components that support
1260 maintenance and are considered a part of the system (including software implementing utilities
1261 such as “ping,” “ls,” “ipconfig,” or hardware and software that implement the monitoring port of
1262 an Ethernet switch).

1263 **REFERENCES**

1264 Source Controls: [MA-03](#), [MA-03\(01\)](#), [MA-03\(02\)](#), [MA-03\(03\)](#)
1265 Supporting Publications: SP 800-88 [50]

1266 **3.7.5. Nonlocal Maintenance**

1267 **REQUIREMENT:** 03.07.05

- 1268 a. Approve and monitor nonlocal maintenance and diagnostic activities.
- 1269 b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal
1270 maintenance and diagnostic sessions.
- 1271 c. Terminate session and network connections when nonlocal maintenance is completed.

1272 **DISCUSSION**

1273 Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate
1274 through an external or internal network. Local maintenance and diagnostic activities are carried
1275 out by individuals who are physically present at the system location and not communicating
1276 across a network connection. Authentication techniques used to establish nonlocal maintenance
1277 and diagnostic sessions reflect the requirements in [03.05.01](#).

1278 **REFERENCES**

1279 Source Control: [MA-04](#)
1280 Supporting Publications: SP 800-63-3 [27], SP 800-88 [50]

1281 **3.7.6. Maintenance Personnel**

1282 **REQUIREMENT:** 03.07.06

- 1283 a. Establish a process for maintenance personnel authorization.
1284 b. Maintain a list of authorized maintenance organizations or personnel.
1285 c. Verify that non-escorted personnel who perform maintenance on the system possess the
1286 required access authorizations.
1287 d. Designate organizational personnel with required access authorizations and technical
1288 competence to supervise the maintenance activities of personnel who do not possess the
1289 required access authorizations.

1290 **DISCUSSION**

1291 Maintenance personnel refers to individuals who perform hardware or software maintenance on
1292 the system, while [03.10.01](#) addresses physical access for individuals whose maintenance duties
1293 place them within the physical protection perimeter of the system. The technical competence of
1294 supervising individuals relates to the maintenance performed on the system, while having
1295 required access authorizations refers to maintenance on and near the system. Individuals who
1296 have not been previously identified as authorized maintenance personnel (e.g., manufacturers,
1297 consultants, systems integrators, and vendors) may require privileged access to the system, such
1298 as when they are required to conduct maintenance with little or no notice. Organizations may
1299 choose to issue temporary credentials to these individuals based on their risk assessments.
1300 Temporary credentials may be for one-time use or for very limited time periods.

1301 **REFERENCES**

1302 Source Control: [MA-05](#)
1303 Supporting Publications: None

1304 **3.8. [Media Protection](#)**

1305 **3.8.1. Media Storage**

1306 **REQUIREMENT:** 03.08.01

1307 Physically control and securely store system media containing CUI until the media are destroyed
1308 or sanitized using approved equipment, techniques, and procedures.

1309 **DISCUSSION**

1310 System media includes digital and non-digital media. Digital media includes diskettes, flash
1311 drives, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and
1312 digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling
1313 stored media includes conducting inventories, establishing procedures to allow individuals to
1314 check out and return media to libraries, and maintaining accountability for stored media. Secure
1315 storage includes a locked drawer, desk, or cabinet or a controlled media library. Controlled areas
1316 provide physical and procedural controls to meet the requirements established for protecting
1317 information and systems. Sanitization techniques (e.g., cryptographically erasing, destroying,
1318 clearing, and purging) prevent the disclosure of CUI to unauthorized individuals. The sanitization
1319 process removes CUI from media such that the information cannot be retrieved or reconstructed.

1320 **REFERENCES**

1321 Source Control: [MP-04](#)
1322 Supporting Publications: SP 800-111 [51]

1323 **3.8.2. Media Access**

1324 **REQUIREMENT:** 03.08.02

1325 Restrict access to CUI on system media.

1326 **DISCUSSION**

1327 System media includes digital and non-digital media. Access to CUI on system media can be
1328 restricted by physically controlling such media, which includes conducting inventories, ensuring
1329 that procedures are in place to allow individuals to check out and return media to the media
1330 library, and maintaining accountability for stored media.

1331 **REFERENCES**

1332 Source Control: [MP-02](#)
1333 Supporting Publications: SP 800-111 [51]

1334 **3.8.3. Media Sanitization**

1335 **REQUIREMENT:** 03.08.03

1336 Sanitize system media containing CUI prior to disposal, release out of organizational control, or
1337 release for reuse.

1338 **DISCUSSION**

1339 Media sanitization applies to digital and non-digital media subject to disposal or reuse, whether or
1340 not the media is considered removable. Examples include digital media in scanners, copiers,
1341 printers, notebook computers, workstations, mobile devices, network components, and non-digital
1342 media. The sanitization process removes CUI from media such that the information cannot be
1343 retrieved or reconstructed. Sanitization techniques (e.g., cryptographically erasing, clearing,
1344 purging, and destroying) prevent the disclosure of CUI to unauthorized individuals when such
1345 media is reused or released for disposal. NARA policies control the sanitization process for media
1346 containing CUI and may require destruction when other methods cannot be applied to the media.

1347 **REFERENCES**

1348 Source Control: [MP-06](#)
1349 Supporting Publications: SP 800-88 [50]

1350 **3.8.4. Media Marking**

1351 **REQUIREMENT:** 03.08.04

1352 Mark system media containing CUI to indicate distribution limitations, handling caveats, and
1353 security markings.

1354 **DISCUSSION**

1355 System media includes digital and non-digital media. Security marking refers to the application or
1356 use of human-readable security attributes. Security labeling refers to the use of security attributes
1357 for internal system data structures. Digital media includes diskettes, magnetic tapes, external or
1358 removable solid state or magnetic drives, flash drives, compact discs, and digital versatile discs.
1359 Non-digital media includes paper and microfilm. CUI is defined by NARA along with marking,
1360 safeguarding, and dissemination requirements for such information.

1361 **REFERENCES**

1362 Source Control: [MP-03](#)
1363 Supporting Publications: None

1364 **3.8.5. Media Transport**

1365 **REQUIREMENT:** 03.08.05

- 1366 a. Protect and control system media containing CUI during transport outside of controlled areas.
1367 b. Maintain accountability of system media containing CUI during transport outside of controlled
1368 areas.

1369 **DISCUSSION**

1370 System media includes digital and non-digital media. Digital media includes flash drives,
1371 diskettes, magnetic tapes, external or removable solid state or magnetic drives, compact discs,
1372 and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are
1373 spaces for which organizations provide physical or procedural measures to meet the requirements
1374 established for protecting information and systems. Media protection during transport can include
1375 cryptography and/or locked containers. Cryptographic mechanisms can provide confidentiality
1376 protections, depending on the mechanisms implemented. Activities associated with media
1377 transport include releasing media for transport, ensuring that media enters the appropriate
1378 transport processes, and the actual transport. Authorized transport and courier personnel may
1379 include individuals external to the organization. Maintaining accountability of media during
1380 transport includes restricting transport activities to authorized personnel and tracking or obtaining
1381 records of transport activities as the media moves through the transportation system to prevent
1382 and detect loss, destruction, or tampering. This requirement is related to [03.13.11](#).

1383 **REFERENCES**

1384 Source Controls: [MP-05](#), [SC-28](#), [SC-28\(01\)](#)
1385 Supporting Publications: SP 800-111 [51]

1386 **3.8.6. Withdrawn**

1387 Incorporated into [03.08.05](#).

1388 **3.8.7. Media Use**

1389 **REQUIREMENT:** 03.08.07

1390 a. Restrict or prohibit the use of [*Assignment: organization-defined types of system media*].

1391 b. Prohibit the use of removable system media without an identifiable owner.

1392 **DISCUSSION**

1393 In contrast to requirement [03.08.01](#), which restricts user access to media, this requirement
1394 restricts the use of certain types of media, such as restricting or prohibiting the use of external
1395 hard drives, flash drives, or smart displays. This requirement also includes any potential
1396 restrictions on the use of removable system media in external systems. Organizations can use
1397 technical and non-technical measures (e.g., policies, procedures, and rules of behavior) to control
1398 the use of system media. For example, organizations may control the use of portable storage
1399 devices by using physical cages on workstations to prohibit access to external ports or disabling
1400 or removing the ability to insert, read, or write to devices.

1401 Organizations may limit the use of portable storage devices to only approved devices, including
1402 devices provided by the organization, devices provided by other approved organizations, and
1403 devices that are not personally owned. Organizations may also control the use of portable storage
1404 devices based on the type of device — prohibiting the use of writeable, portable devices — and
1405 implement this restriction by disabling or removing the capability to write to such devices. Limits
1406 on the use of organization-controlled system media in external systems include restrictions on
1407 how the media may be used and under what conditions. Requiring identifiable owners (e.g.,
1408 individuals, organizations, or projects) for removable system media reduces the risk of using such
1409 technologies by allowing organizations to assign responsibility and accountability for addressing
1410 known vulnerabilities in the media (e.g., insertion of malicious code).

1411 **REFERENCES**

1412 Source Control: [MP-07](#)

1413 Supporting Publications: SP 800-111 [51]

1414 **3.8.8. Withdrawn**

1415 Incorporated into [03.08.07](#).

1416 **3.8.9. System Backup – Cryptographic Protection**

1417 **REQUIREMENT:** 03.08.09

1418 Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup
1419 storage locations.

1420 **DISCUSSION**

1421 Backup storage locations may include system-level information and user-level information.
1422 System-level information includes system state information, operating system software,

1423 application software, and licenses. User-level information includes information other than
1424 system-level information. Hardware-enabled security technologies (e.g., hardware security
1425 modules [HSM]) can be used to enhance cryptographic protection for backup information. HSM
1426 devices safeguard and manage cryptographic keys and provide cryptographic processing.
1427 Cryptographic operations (e.g., encryption, decryption, and signature generation/verification) are
1428 typically hosted on the HSM device, and many implementations provide hardware-accelerated
1429 mechanisms for cryptographic operations. This requirement is related to [03.13.11](#).

1430 REFERENCES

1431 Source Control: [CP-09\(08\)](#)
1432 Supporting Publications: SP 800-34 [52], SP 800-130 [53], SP 800-152 [54]

1433 3.9. [Personnel Security](#)

1434 3.9.1. Personnel Screening

1435 **REQUIREMENT:** 03.09.01

- 1436 a. Screen individuals prior to authorizing access to the system.
1437 b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions*
1438 *requiring rescreening*].

1439 DISCUSSION

1440 Personnel security screening activities involve the assessment of an individual's conduct,
1441 integrity, judgment, loyalty, reliability, and stability (i.e., the individual's trustworthiness) prior to
1442 authorizing access to the system or when elevating system access. The screening and rescreening
1443 activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and
1444 criteria established for the level of access required for the assigned position.

1445 REFERENCES

1446 Source Control: [PS-03](#)
1447 Supporting Publications: SP 800-181 [34]

1448 3.9.2. Personnel Termination and Transfer

1449 **REQUIREMENT:** 03.09.02

- 1450 a. When individual employment is terminated:
- 1451 1. Disable system access within [*Assignment: organization-defined time period*];
 - 1452 2. Terminate or revoke authenticators and credentials associated with the individual; and
 - 1453 3. Retrieve security-related system property.
- 1454 b. When individuals are reassigned or transferred to other positions in the organization:
- 1455 1. Review and confirm the ongoing operational need for current logical and physical access
1456 authorizations to the system and facility;
 - 1457 2. Initiate [*Assignment: organization-defined transfer or reassignment actions*] within
1458 [*Assignment: organization-defined time period following the transfer or reassignment*
1459 *action*]; and

- 1460 3. Modify access authorization to correspond with any changes in operational need.

1461 **DISCUSSION**

1462 Security-related system property includes hardware authentication tokens, system administration
1463 technical manuals, keys, identification cards, and building passes. Exit interviews ensure that
1464 terminated individuals understand the security constraints imposed by being former employees
1465 and that accountability is achieved for the organizational property. Security topics at exit
1466 interviews include reminding individuals of potential limitations on future employment and
1467 nondisclosure agreements. Exit interviews may not always be possible for some individuals,
1468 including in cases related to the unavailability of supervisors, illnesses, or job abandonment.

1469 The timely execution of termination actions is essential for individuals who have been terminated
1470 for cause. Organizations may consider disabling the accounts of individuals who are being
1471 terminated prior to the individuals being notified. This requirement applies to the reassignment or
1472 transfer of individuals when the personnel action is permanent or of such extended duration as to
1473 require protection. Protections that may be required for transfers or reassignments to other
1474 positions within organizations include returning old and issuing new identification cards, keys,
1475 and building passes; changing system access authorizations (i.e., privileges); closing system
1476 accounts and establishing new accounts; and providing access to official records to which
1477 individuals had access at previous work locations in previous system accounts.

1478 **REFERENCES**

1479 Source Controls: [PS-04](#), [PS-05](#)
1480 Supporting Publications: None

1481 **3.10. [Physical Protection](#)**

1482 **3.10.1. Physical Access Authorizations**

1483 **REQUIREMENT:** 03.10.01

- 1484 a. Develop, approve, and maintain a list of individuals with authorized access to the physical
1485 location where the system resides.
- 1486 b. Issue authorization credentials for physical access.
- 1487 c. Review the physical access list periodically.
- 1488 d. Remove individuals from the physical access list when access is no longer required.

1489 **DISCUSSION**

1490 A facility can include one or more physical locations containing systems or system components
1491 that process, store, or transmit CUI. Physical access authorizations apply to employees and
1492 visitors. Individuals with permanent physical access authorization credentials are not considered
1493 visitors. Authorization credentials include identification badges, identification cards, and smart
1494 cards. Organizations determine the strength of the authorization credentials consistent with
1495 applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.
1496 Physical access authorizations may not be necessary to access certain areas within facilities that
1497 are designated as publicly accessible.

1498 **REFERENCES**

1499 Source Control: [PE-02](#)
1500 Supporting Publications: None

1501 **3.10.2. Monitoring Physical Access**

1502 **REQUIREMENT:** 03.10.02

- 1503 a. Monitor physical access to the location where the system resides to detect and respond to
1504 physical security incidents.
1505 b. Review physical access logs periodically.

1506 **DISCUSSION**

1507 A facility can include one or more physical locations containing systems or system components
1508 that process, store, or transmit CUI. Physical access monitoring includes publicly accessible
1509 areas within organizational facilities. Examples of physical access monitoring include the
1510 employment of guards, video surveillance equipment (i.e., cameras), and sensor devices.
1511 Reviewing physical access logs can help identify suspicious activity, anomalous events, or
1512 potential threats. The reviews can be supported by audit logging controls if the access logs are
1513 part of an automated system. Incident response capabilities include investigations of physical
1514 security incidents and responses to those incidents. Incidents include security violations or
1515 suspicious physical access activities, such as access outside of normal work hours, repeated
1516 access to areas not normally accessed, access for unusual lengths of time, and out-of-sequence
1517 access.

1518 **REFERENCES**

1519 Source Control: [PE-06](#)
1520 Supporting Publications: None

1521 **3.10.3. Withdrawn**

1522 Incorporated into [03.10.07](#).

1523 **3.10.4. Withdrawn**

1524 Incorporated into [03.10.07](#).

1525 **3.10.5. Withdrawn**

1526 Incorporated into [03.10.07](#).

1527 **3.10.6. Alternate Work Site**

1528 **REQUIREMENT:** 03.10.06

- 1529 a. Determine alternate work sites allowed for use by employees.
1530 b. Employ the following security requirements at alternate work sites: [*Assignment:*
1531 *organization-defined security requirements*].

1532 **DISCUSSION**
1533 Alternate work sites include the private residences of employees or other facilities designated
1534 by the organization. Alternate work sites can provide readily available alternate locations during
1535 contingency operations. Organizations can define different security requirements for specific
1536 alternate work sites or types of sites, depending on the work-related activities conducted at the
1537 sites. Assessing the effectiveness of the requirements and providing a means to communicate
1538 incidents at alternate work sites supports the contingency planning activities of organizations.

1539 **REFERENCES**
1540 Source Control: [PE-17](#)
1541 Supporting Publications: SP 800-46 [14], SP 800-114 [20]

1542 **3.10.7. Physical Access Control**

- 1543 **REQUIREMENT:** 03.10.07
- 1544 a. Control physical access at the location where the system resides by:
 - 1545 1. Verifying individual physical access authorizations before granting access; and
 - 1546 2. Controlling ingress and egress with physical access control systems/devices or guards.
 - 1547 b. Maintain physical access audit logs for entry or exit points.
 - 1548 c. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances*
1549 *requiring visitor escorts and control of visitor activity*].
 - 1550 d. Secure keys, combinations, and other physical access devices.

1551 **DISCUSSION**
1552 This requirement addresses physical locations containing systems or system components that
1553 process, store, or transmit CUI. Organizations determine the types of guards needed, including
1554 professional security staff or administrative staff. Physical access devices include keys, locks,
1555 combinations, biometric readers, and card readers. Physical access control systems comply with
1556 applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.
1557 Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural,
1558 automated, or some combination thereof. Physical access points can include exterior access
1559 points, interior access points to systems that require supplemental access controls, or both.
1560 Physical access control applies to employees and visitors. Individuals with permanent physical
1561 access authorizations are not considered visitors.

1562 **REFERENCES**
1563 Source Control: [PE-03](#)
1564 Supporting Publications: None

1565 **3.10.8. Access Control for Transmission and Output Devices**

- 1566 **REQUIREMENT:** 03.10.08
- 1567 a. Control physical access to system distribution and transmission lines in organizational
1568 facilities.
 - 1569 b. Control physical access to output devices to prevent unauthorized individuals from
1570 obtaining access to CUI.

1571 **DISCUSSION**
1572 Safeguarding measures applied to system distribution and transmission lines prevent accidental
1573 damage, disruption, and physical tampering. Such measures may also be necessary to prevent
1574 eavesdropping or the modification of unencrypted transmissions. Safeguarding measures used
1575 to control physical access to system distribution and transmission lines include disconnected or
1576 locked spare jacks, locked wiring closets, protecting cabling with conduit or cable trays, and
1577 wiretapping sensors. Controlling physical access to output devices includes placing output
1578 devices in locked rooms or other secured areas with keypad or card reader access controls and
1579 allowing access to authorized individuals only, placing output devices in locations that can be
1580 monitored by personnel, installing monitor or screen filters, and using headphones. Examples of
1581 output devices include monitors, printers, scanners, audio devices, facsimile machines, and
1582 copiers.

1583 **REFERENCES**
1584 Source Controls: [PE-04](#), [PE-05](#)
1585 Supporting Publications: None

1586 **3.11. [Risk Assessment](#)**

1587 **3.11.1. Risk Assessment**

- 1588 **REQUIREMENT:** 03.11.01
- 1589 a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the
 - 1590 processing, storage, or transmission of CUI.
 - 1591 b. Update risk assessments periodically.

1592 **DISCUSSION**
1593 Establishing the system boundary is a prerequisite to assessing the risk of unauthorized
1594 disclosure of CUI. Risk assessments consider threats, vulnerabilities, likelihood, and adverse
1595 impacts to organizational operations and assets based on the operation and use of the system
1596 and the unauthorized disclosure of CUI. Risk assessments also consider risks from external
1597 parties (e.g., service providers, contractors operating systems on behalf of the organization,
1598 individuals accessing systems, outsourcing entities). Risk assessments can be conducted at the
1599 organization level, the mission or business process level, or the system level and at any phase in
1600 the system development life cycle. Risk assessments include supply chain-related risks
1601 associated with suppliers or contractors and the system, system component, or system service
1602 that they provide.

1603 **REFERENCES**
1604 Source Controls: [RA-03](#), [RA-03\(01\)](#), [SR-06](#)
1605 Supporting Publications: SP 800-30 [55], SP 800-161 [33]

1606 **3.11.2. Vulnerability Monitoring and Scanning**

- 1607 **REQUIREMENT:** 03.11.02
- 1608 a. Monitor and scan for vulnerabilities in the system periodically and when new vulnerabilities
 - 1609 affecting the system are identified.

- 1610 b. Remediate system vulnerabilities within [*Assignment: organization-defined response times*].
- 1611 c. Update system vulnerabilities to be scanned periodically and when new vulnerabilities are
- 1612 identified and reported.

1613 **DISCUSSION**

1614 Organizations determine the required vulnerability scanning for system components and ensure
1615 that potential sources of vulnerabilities (e.g., networked printers, scanners, and copiers) are not
1616 overlooked. Vulnerability analyses for custom software may require additional approaches, such
1617 as static analysis, dynamic analysis, or binary analysis. Organizations can use these approaches
1618 in source code reviews and tools (e.g., static analysis tools, web-based application scanners,
1619 binary analyzers). Vulnerability scanning includes scanning for patch levels; scanning for
1620 functions, ports, protocols, and services that should not be accessible to users or devices; and
1621 scanning for improperly configured or incorrectly operating flow control mechanisms.

1622 To facilitate interoperability, organizations consider using products that are Security Content
1623 Automated Protocol (SCAP)-validated and that employ the Extensible Configuration Checklist
1624 Description Format (XCCDF). Organizations also consider using scanning tools that express
1625 vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and
1626 that employ the Open Vulnerability Assessment Language (OVAL). Sources for vulnerability
1627 information also include the Common Weakness Enumeration (CWE) listing, the National
1628 Vulnerability Database (NVD), and the Common Vulnerability Scoring System (CVSS).

1629 **REFERENCES**

1630 Source Controls: [RA-05](#), [RA-05\(02\)](#)
1631 Supporting Publications: SP 800-40 [56], SP 800-53A [57], SP 800-70 [44], SP 800-115 [58],
1632 SP 800-126 [45]

1633 **3.11.3. Withdrawn**

1634 Incorporated into [03.11.02](#).

1635 **3.12. [Security Assessment and Monitoring](#)**

1636 **3.12.1. Security Assessment**

1637 **REQUIREMENT:** 03.12.01

1638 Assess the security requirements for the system and its environment of operation periodically to
1639 determine if the requirements have been satisfied.

1640 **DISCUSSION**

1641 By assessing the security requirements, organizations determine whether the necessary
1642 safeguards and countermeasures are implemented correctly, operating as intended, and
1643 producing the desired outcome. Security assessments identify weaknesses and deficiencies in
1644 the system and provide the essential information needed to make risk-based decisions. Security
1645 assessment reports document assessment results in sufficient detail as deemed necessary by the
1646 organization to determine the accuracy and completeness of the reports. Security assessment
1647 results are provided to the individuals or roles appropriate for the types of assessments being
1648 conducted.

1649 **REFERENCES**

1650 Source Control: [CA-02](#)
1651 Supporting Publications: SP 800-53 [8], SP 800-53A [57], SP 800-37 [59], SP 800-115 [58]

1652 **3.12.2. Plan of Action and Milestones**

1653 **REQUIREMENT:** 03.12.02

- 1654 a. Develop a plan of action and milestones for the system:
- 1655 1. To document the planned remediation actions to correct weaknesses or deficiencies
1656 noted during security assessments; and
 - 1657 2. To reduce or eliminate known system vulnerabilities.
- 1658 b. Update the existing plan of action and milestones periodically based on the findings from
1659 security assessments, independent audits or reviews, and continuous monitoring activities.

1660 **DISCUSSION**

1661 Plans of action and milestones (POAMs) are important documents in organizational security
1662 programs. Organizations use POAMs to describe how unsatisfied security requirements will be
1663 met and how planned mitigations will be implemented. Organizations can document system
1664 security plans and POAMs as separate or combined documents and in any format. Federal
1665 agencies may consider system security plans and POAMs as inputs to risk-based decisions on
1666 whether to process, store, or transmit CUI on a system hosted by a nonfederal organization.

1667 **REFERENCES**

1668 Source Control: [CA-05](#)
1669 Supporting Publications: SP 800-37 [59]

1670 **3.12.3. Continuous Monitoring**

1671 **REQUIREMENT:** 03.12.03

1672 Develop and implement a system-level continuous monitoring strategy that includes ongoing
1673 monitoring and security assessments.

1674 **DISCUSSION**

1675 Continuous monitoring at the system level facilitates ongoing awareness of the system security
1676 posture to support risk management decisions. The terms *continuous* and *ongoing* imply that
1677 organizations assess and monitor their systems at a frequency that is sufficient to support risk-
1678 based decisions. Different types of security requirements may require different monitoring
1679 frequencies.

1680 **REFERENCES**

1681 Source Control: [CA-07](#)
1682 Supporting Publications: SP 800-37 [59], SP 800-39 [60], SP 800-53A [57], SP 800-115 [58],
1683 SP 800-137 [49]

1684 **3.12.4. Withdrawn**

1685 Incorporated into [03.15.02](#).

1686 **3.12.5. Information Exchange**

1687 **REQUIREMENT:** 03.12.05

- 1688 a. Approve and manage the exchange of CUI between the system and other systems using
1689 [*Selection (one or more): interconnection security agreements; information exchange*
1690 *security agreements; memoranda of understanding or agreement; service level*
1691 *agreements; user agreements; nondisclosure agreements*].
- 1692 b. Document, as part of the exchange agreements, interface characteristics, security
1693 requirements, and responsibilities for each system.
- 1694 c. Review and update the exchange agreements periodically.

1695 **DISCUSSION**

1696 The types of agreements selected are based on factors such as the relationship between the
1697 organizations exchanging information (e.g., government to government, government to
1698 business, business to business, government or business to service provider, government or
1699 business to individual) and the level of access to the organizational system by users of the other
1700 system. Types of agreements can include interconnection security agreements, information
1701 exchange security agreements, memoranda of understanding or agreement, service-level
1702 agreements, or other types of agreements. Organizations may incorporate agreement
1703 information into formal contracts, especially for information exchanges established between
1704 federal agencies and nonfederal organizations (e.g., service providers, contractors, system
1705 developers, and system integrators). Examples of the types of information contained in
1706 exchange agreements include the interface characteristics, security requirements, controls, and
1707 responsibilities for each system.

1708 **REFERENCES**

1709 Source Control: [CA-03](#)
1710 Supporting Publications: SP 800-47 [83]

1711 **3.13. [System and Communications Protection](#)**

1712 **3.13.1. Boundary Protection**

1713 **REQUIREMENT:** 03.13.01

- 1714 a. Monitor and control communications at the external managed interfaces to the system and
1715 at key internal managed interfaces within the system.
- 1716 b. Implement subnetworks for publicly accessible system components that are physically or
1717 logically separated from internal networks.
- 1718 c. Connect to external systems only through managed interfaces consisting of boundary
1719 protection devices arranged in accordance with an organizational security architecture.

1720 **DISCUSSION**
1721 Managed interfaces include gateways, routers, firewalls, network-based malicious code
1722 analysis, virtualization systems, and encrypted tunnels implemented within a security
1723 architecture. Subnetworks that are either physically or logically separated from internal
1724 networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces
1725 within organizational systems includes restricting external web traffic to designated web servers
1726 within managed interfaces, prohibiting external traffic that appears to be spoofing internal
1727 addresses, and prohibiting internal traffic that appears to be spoofing external addresses.

1728 **REFERENCES**
1729 Source Control: [SC-07](#)
1730 Supporting Publications: SP 800-41 [64], SP 800-125B [65], SP 800-160-1 [11], SP 800-189
1731 [67], SP 800-207 [66]

1732 **3.13.2. Withdrawn**

1733 Recategorized as NCO.

1734 **3.13.3. Withdrawn**

1735 Addressed by [03.01.01](#), [03.01.02](#), [03.01.03](#), [03.01.04](#), [03.01.05](#), [03.01.06](#), [03.01.07](#).

1736 **3.13.4. Information in Shared System Resources**

1737 **REQUIREMENT:** 03.13.04

1738 Prevent unauthorized and unintended information transfer via shared system resources.

1739 **DISCUSSION**

1740 Preventing unauthorized and unintended information transfer via shared system resources stops
1741 information produced by the actions of prior users or roles (or actions of processes acting on
1742 behalf of prior users or roles) from being available to current users or roles (or current processes
1743 acting on behalf of current users or roles) that obtain access to shared system resources after
1744 those resources have been released back to the system. Information in shared system resources
1745 also applies to encrypted representations of information. In other contexts, the control of
1746 information in shared system resources is referred to as object reuse and residual information
1747 protection. Information in shared system resources does not address information remanence,
1748 which refers to the residual representation of data that has been nominally deleted, covert
1749 channels (including storage and timing channels) in which shared system resources are
1750 manipulated to violate information flow restrictions, or components within systems for which
1751 there are only single users or roles.

1752 **REFERENCES**
1753 Source Control: [SC-04](#)
1754 Supporting Publications: None

1755 **3.13.5. Withdrawn**

1756 Incorporated into [03.13.01](#).

1757 **3.13.6. Network Communications – Deny by Default – Allow by Exception**

1758 **REQUIREMENT:** 03.13.06

1759 Deny network communications traffic by default and allow network communications traffic by
1760 exception.

1761 **DISCUSSION**

1762 This requirement applies to inbound and outbound network communications traffic at the
1763 system boundary and at identified points within the system. A deny-all, allow-by-exception
1764 network communications traffic policy ensures that only essential and approved connections are
1765 allowed.

1766 **REFERENCES**

1767 Source Control: [SC-07\(05\)](#)

1768 Supporting Publications: SP 800-41 [64], SP 800-77 [18], SP 800-189 [67]

1769 **3.13.7. Withdrawn**

1770 Addressed by [03.01.12](#), [03.04.02](#) and [03.04.06](#).

1771 **3.13.8. Transmission and Storage Confidentiality**

1772 **REQUIREMENT:** 03.13.08

1773 Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during
1774 transmission and while in storage.

1775 **DISCUSSION**

1776 This requirement applies to internal and external networks and any system components that can
1777 transmit CUI, including servers, notebook computers, desktop computers, mobile devices,
1778 printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths
1779 are susceptible to interception and modification. Encryption protects CUI from unauthorized
1780 disclosure during transmission and while in storage. Cryptographic mechanisms that protect the
1781 confidentiality of CUI during transmission include TLS and IPsec. Information in storage (i.e.,
1782 information at rest) refers to the state of CUI when it is not in process or in transit and resides
1783 on internal or external storage devices, storage area network devices, and databases. Protecting
1784 CUI in storage does not focus on the type of storage device or the frequency of access to that
1785 device but rather on the state of the information. This requirement relates to [03.13.11](#).

1786 **REFERENCES**

1787 Source Controls: [SC-08](#), [SC-08\(01\)](#), [SC-28](#), [SC-28\(01\)](#)

1788 Supporting Publications: FIPS 140-3 [38], FIPS 197 [68], SP 800-46 [14], SP 800-52 [69], SP
1789 800-56A [73], SP 800-56B [74], SP 800-56C [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-
1790 57-3 [17], SP 800-77 [18], SP 800-111 [51], SP 800-113 [19], SP 800-114 [20], SP 800-121
1791 [21], SP 800-124 [28], SP 800-177 [70]

1792 **3.13.9. Network Disconnect**

1793 **REQUIREMENT:** 03.13.09

1794 Terminate network connections associated with communications sessions at the end of the
1795 sessions or after periods of inactivity.

1796 **DISCUSSION**

1797 This requirement applies to internal and external networks. Terminating network connections
1798 associated with communications sessions includes deallocating TCP/IP addresses or port pairs
1799 at the operating system level or deallocating networking assignments at the application level if
1800 multiple application sessions are using a single network connection. Time periods of inactivity
1801 may be established by organizations and include time periods by type of network access or for
1802 specific network accesses.

1803 **REFERENCES**

1804 Source Control: [SC-10](#)
1805 Supporting Publications: None

1806 **3.13.10. Cryptographic Key Establishment and Management**

1807 **REQUIREMENT:** 03.13.10

1808 Establish and manage cryptographic keys in the system in accordance with the following key
1809 management requirements: [*Assignment: organization-defined requirements for key*
1810 *establishment and management*].

1811 **DISCUSSION**

1812 Cryptographic key establishment and management include key generation, distribution,
1813 storage, access, rotation, and destruction. Cryptographic keys can be established and managed
1814 using either manual procedures or automated mechanisms supported by manual procedures.
1815 Organizations satisfy key establishment and management requirements in accordance with
1816 applicable federal laws, Executive Orders, policies, directives, regulations, and standards that
1817 specify appropriate options, levels, and parameters. This requirement is related to [03.13.11](#).

1818 **REFERENCES**

1819 Source Control: [SC-12](#)
1820 Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C
1821 [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]

1822 **3.13.11. Cryptographic Protection**

1823 **REQUIREMENT:** 03.13.11

1824 Implement the following types of cryptography when used to protect the confidentiality of CUI:
1825 [*Assignment: organization-defined types of cryptography*].

1826 **DISCUSSION**

1827 Cryptography is implemented in accordance with applicable laws, Executive Orders,
1828 directives, regulations, policies, standards, and guidelines.

1829 **REFERENCES**

1830 Source Control: [SC-13](#)

1831 Supporting Publications: FIPS 140-3 [38]

1832 **3.13.12. Collaborative Computing Devices and Applications**

1833 **REQUIREMENT:** 03.13.12

- 1834 a. Prohibit remote activation of collaborative computing devices and applications.
1835 b. Provide an explicit indication of use to users physically present at the devices.

1836 **DISCUSSION**

1837 Collaborative computing devices include white boards, microphones, and cameras. Indication
1838 of use includes notifying users (e.g., a pop-up menu stating that recording is in progress, or
1839 that the microphone has been turned on) when collaborative computing devices are activated.
1840 Dedicated video conferencing systems, which typically rely on one of the participants calling
1841 or connecting to the other party to activate the video conference, are excluded. Solutions to
1842 prevent device usage include webcam covers and buttons to disable microphones.

1843 **REFERENCES**

1844 Source Control: [SC-15](#)
1845 Supporting Publications: None

1846 **3.13.13. Mobile Code**

1847 **REQUIREMENT:** 03.13.13

- 1848 a. Define acceptable mobile code and mobile code technologies.
1849 b. Authorize, monitor, and control the use of mobile code.

1850 **DISCUSSION**

1851 Mobile code includes software programs or parts of programs obtained from remote systems,
1852 transmitted across a network, and executed on a local system without explicit installation or
1853 execution by the recipient. Decisions regarding the use of mobile code within the system are
1854 based on the potential for the code to cause damage to the system if used maliciously. Mobile
1855 code technologies include Java applets, JavaScript, HTML5, VBScript, and WebGL. Usage
1856 restrictions and implementation guidelines apply to the selection and use of mobile code
1857 installed on servers and mobile code downloaded and executed on individual workstations and
1858 devices, including notebook computers, smart phones, and smart devices. Mobile code policy
1859 and procedures address the actions taken to prevent the development, acquisition, and use of
1860 unacceptable mobile code within the system, including requiring mobile code to be digitally
1861 signed by a trusted source.

1862 **REFERENCES**

1863 Source Control: [SC-18](#)
1864 Supporting Publications: SP 800-28 [71]

1865 **3.13.14. Withdrawn**

1866 Technology-specific.

1867 **3.13.15. Session Authenticity**

1868 **REQUIREMENT:** 03.13.15

1869 Protect the authenticity of communications sessions.

1870 **DISCUSSION**

1871 Protecting session authenticity addresses communications protection at the session level, not
1872 at the packet level. Such protection establishes grounds for confidence at both ends of the
1873 communications sessions in the ongoing identities of other parties and the validity of the
1874 transmitted information. Authenticity protection includes protecting against “adversary-in-the-
1875 middle” attacks, session hijacking, and the insertion of false information into sessions.

1876 **REFERENCES**

1877 Source Control: [SC-23](#)

1878 Supporting Publications: SP 800-52 [69], SP 800-77 [18], SP 800-95 [72], SP 800-113 [19]

1879 **3.13.16. Withdrawn**

1880 Incorporated into [03.13.08](#).

1881 **3.14. [System and Information Integrity](#)**

1882 **3.14.1. Flaw Remediation**

1883 **REQUIREMENT:** 03.14.01

1884 a. Identify, report, and correct system flaws.

1885 b. Install security-relevant software and firmware updates within [*Assignment: organization-*
1886 *defined time period*] of the release of the updates.

1887 **DISCUSSION**

1888 Organizations identify systems that are affected by announced software and firmware flaws,
1889 including potential vulnerabilities that result from those flaws, and report this information to
1890 designated personnel with information security responsibilities. Security-relevant updates
1891 include patches, service packs, hot fixes, and anti-virus signatures. Organizations address the
1892 flaws discovered during security assessments, continuous monitoring, incident response
1893 activities, and system error handling. Organizations can take advantage of available resources,
1894 such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures
1895 (CVE) databases, in remediating the flaws discovered in organizational systems. Organization-
1896 defined time periods for updating security-relevant software and firmware may vary based on a
1897 variety of factors, including the criticality of the update (i.e., severity of the vulnerability related
1898 to the discovered flaw). Some types of flaw remediation may require more testing than other
1899 types of remediation.

1900 **REFERENCES**

1901 Source Control: [SI-02](#)

1902 Supporting Publications: SP 800-39 [60], SP 800-40 [56], SP 800-128 [41]

1903 **3.14.2. Malicious Code Protection**

1904 **REQUIREMENT: 03.14.02**

- 1905 a. Implement malicious code protection mechanisms at designated locations within the system
1906 to detect and eradicate malicious code.
- 1907 b. Update malicious code protection mechanisms as new releases are available in accordance
1908 with configuration management policy and procedures.
- 1909 c. Configure malicious code protection mechanisms to:
- 1910 1. Perform scans of the system [*Assignment: organization-defined frequency*] and real-
1911 time scans of files from external sources at endpoints or network entry and exit points
1912 as the files are downloaded, opened, or executed; and
 - 1913 2. Block malicious code, quarantine malicious code, or take other actions in response to
1914 malicious code detection.

1915 **DISCUSSION**

1916 Malicious code insertions occur through the exploitation of system vulnerabilities. Periodic
1917 scans of the system and real-time scans of files from external sources as files are downloaded,
1918 opened, or executed can detect malicious code. Malicious code can be inserted into the system
1919 in many ways, including by email, the Internet, and portable storage devices. Malicious code
1920 includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various
1921 formats, contained in compressed or hidden files, or hidden in files using techniques such as
1922 steganography. In addition to the above technologies, pervasive configuration management,
1923 comprehensive software integrity controls, and anti-exploitation software may be effective in
1924 preventing the execution of unauthorized code. Malicious code may be present in commercial
1925 off-the-shelf software and custom-built software and could include logic bombs, backdoors, and
1926 other types of attacks that could affect organizational mission and business functions.

1927 If malicious code cannot be detected by detection methods or technologies, organizations can
1928 rely on secure coding practices, configuration management and control, trusted procurement
1929 processes, and monitoring practices to help ensure that the software only performs intended
1930 functions. Organizations may determine that different actions are warranted in response to the
1931 detection of malicious code. For example, organizations can define actions to be taken in
1932 response to malicious code detection during scans, the detection of malicious downloads, or the
1933 detection of maliciousness when attempting to open or execute files.

1934 **REFERENCES**

1935 Source Control: [SI-03](#)
1936 Supporting Publications: SP 800-83 [76], SP 800-125B [65], SP 800-177 [70]

1937 **3.14.3. Security Alerts, Advisories, and Directives**

1938 **REQUIREMENT: 03.14.03**

- 1939 a. Receive system security alerts, advisories, and directives from external organizations on an
1940 ongoing basis.
- 1941 b. Generate and disseminate internal system security alerts, advisories, and directives, as
1942 necessary.
- 1943 c. Implement security directives in accordance with established time frames.

1944

DISCUSSION

1945
1946
1947
1948
1949
1950
1951
1952
1953
1954

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

1955

REFERENCES

1956
1957

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

1958

3.14.4. Withdrawn

1959

Incorporated into [03.14.02](#).

1960

3.14.5. Withdrawn

1961

Addressed by [03.14.02](#).

1962

3.14.6. System Monitoring

1963
1964
1965
1966
1967
1968
1969

REQUIREMENT: 03.14.06

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

1970

DISCUSSION

1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981

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

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

1982 The granularity of monitoring the information collected is based on organizational monitoring
1983 objectives and the capability of the system to support such objectives.

1984 Systems connections can be network, remote, or local. A network connection is any connection
1985 with a device that communicates through a network (e.g., local area network, the internet). A
1986 remote connection is any connection with a device that communicates through an external
1987 network (e.g., the internet). Network, remote, and local connections can be either wired or
1988 wireless.

1989 Unusual or unauthorized activities or conditions related to inbound and outbound
1990 communications traffic include internal traffic that indicates the presence of malicious code in
1991 the system or propagating among system components, the unauthorized export of information,
1992 or signaling to external systems. Evidence of malicious code is used to identify a potentially
1993 compromised system. System monitoring requirements, including the need for types of system
1994 monitoring, may be referenced in other requirements.

1995 **REFERENCES**

1996 Source Controls: [SI-04](#), [SI-04\(04\)](#)
1997 Supporting Publications: SP 800-61 [47], SP 800-83 [76], SP 800-92 [35], SP 800-94 [29], SP
1998 800-137 [49], SP 800-177 [70]

1999 **3.14.7. Withdrawn**

2000 Incorporated into [03.14.06](#).

2001 **3.14.8. Information Management and Retention**

2002 **REQUIREMENT:** 03.14.08

2003 Manage and retain CUI within the system and CUI output from the system in accordance with
2004 applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and
2005 operational requirements.

2006 **DISCUSSION**

2007 Federal agencies consider data retention requirements for nonfederal organizations. Retaining
2008 CUI on nonfederal systems after contracts or agreements have concluded increases the attack
2009 surface for those systems and the risk of the information being compromised. NARA provides
2010 federal policy and guidance on records retention and schedules.

2011 **REFERENCES**

2012 Source Control: [SI-12](#)
2013 Supporting Publications: None

2014 **3.15. [Planning](#)**

2015 **3.15.1. Policy and Procedures**

2016 **REQUIREMENT:** 03.15.01

2017 a. Develop, document, and disseminate to organizational personnel or roles, policies and
2018 procedures needed to implement security requirements.

- 2019 b. Review and update policies and procedures periodically.

2020 **DISCUSSION**

2021 This requirement addresses policies and procedures for the protection of CUI. Policies and
2022 procedures contribute to security assurance and should address each family of the CUI security
2023 requirements. Policies can be included as part of the generalized organizational security policy
2024 or be represented by separate policies that address each family of requirements. Procedures
2025 describe how policies are implemented and can be directed at the individual or role that is the
2026 object of the procedure. Procedures can be documented in system security plans or in one or
2027 more separate documents.

2028 **REFERENCES**

2029 Source Controls: [AC-01](#), [AT-01](#), [AU-01](#), [CA-01](#), [CM-01](#), [IA-01](#), [IR-01](#), [MA-01](#), [MP-01](#), [PE-01](#),
2030 [PL-01](#), [PS-01](#), [RA-01](#), [SA-01](#), [SC-01](#), [SI-01](#), [SR-01](#)
2031 Supporting Publications: SP 800-12 [61], SP 800-100 [62]

2032 **3.15.2. System Security Plan**

2033 **REQUIREMENT:** 03.15.02

- 2034 a. Develop a system security plan that:
- 2035 1. Defines the constituent system components;
 - 2036 2. Describes the system operating environment;
 - 2037 3. Describes specific threats to the system that are of concern to the organization;
 - 2038 4. Provides an overview of the security requirements for the system;
 - 2039 5. Identifies connections to other systems;
 - 2040 6. Identifies individuals that fulfill system roles and responsibilities; and
 - 2041 7. Includes other relevant information necessary for the protection of CUI.
- 2042 b. Review and update the system security plan periodically.
- 2043 c. Protect the system security plan from unauthorized disclosure.

2044 **DISCUSSION**

2045 System security plans provide key characteristics of the system that is processing, storing, and
2046 transmitting CUI and how the system and information are protected. System security plans
2047 contain sufficient information to enable a design and implementation that is unambiguously
2048 compliant with the intent of the plans and the subsequent determinations of risk if the plan is
2049 implemented as intended. System security plans can be a collection of documents, including
2050 documents that already exist. Effective system security plans make use of references to policies,
2051 procedures, and additional documents (e.g., design specifications) where detailed information
2052 can be obtained. This reduces the documentation requirements associated with security
2053 programs and maintains security information in other established management or operational
2054 areas related to enterprise architecture, the system development life cycle, systems engineering,
2055 and acquisition.

2056 **REFERENCES**

2057 Source Control: [PL-02](#)

2058 Supporting Publications: SP 800-18 [63]

2059 **3.15.3. Rules of Behavior**

2060 **REQUIREMENT:** 03.15.03

- 2061 a. Establish and provide to individuals requiring access to the system, rules that describe their
2062 responsibilities and expected behavior for handling CUI and system usage.
- 2063 b. Receive a documented acknowledgement from individuals indicating that they have read,
2064 understand, and agree to abide by the rules of behavior before authorizing access to CUI
2065 and the system.
- 2066 c. Review and update the rules of behavior periodically.

2067 **DISCUSSION**

2068 Rules of behavior represent a type of access agreement for system users. Organizations consider
2069 rules of behavior for the handling of CUI based on individual user roles and responsibilities and
2070 differentiate between rules that apply to privileged users and rules that apply to general users.

2071 **REFERENCES**

2072 Source Control: [PL-04](#)
2073 Supporting Publications: SP 800-18 [63]

2074 **3.16. System and Services Acquisition**

2075 **3.16.1. Acquisition Process**

2076 **REQUIREMENT:** 03.16.01

2077 Include the following security requirements, explicitly or by reference, in the acquisition contract
2078 for the system, system component, or system service: [*Assignment: organization-defined*
2079 *security requirements*].

2080 **DISCUSSION**

2081 Security requirements include security functional and security assurance requirements. Security
2082 functional requirements are typically derived from mission or business requirements as well as
2083 requirements stated in laws, regulations, policies, and standards. The derived requirements can
2084 include security capabilities, functions, and mechanisms. Assurance requirements can include
2085 development processes, procedures, methodologies, and the evidence from development and
2086 assessment activities that provide grounds for confidence that the required functionality is
2087 implemented and possesses the required strength of mechanism. Strength of mechanism
2088 requirements associated with such capabilities, functions, and mechanisms include degree of
2089 correctness, completeness, resistance to tampering or bypass, and resistance to direct attack.
2090 This requirement is related to [03.16.03](#) and [03.17.02](#).

2091 **REFERENCES**

2092 Source Control: [SA-04](#)
2093 Supporting Publications: SP 800-160-1 [11], SP 800-160-2 [10], SP 800-161 [33]

2094 **3.16.2. Unsupported System Components**

2095 **REQUIREMENT:** 03.16.02

- 2096 a. Replace system components when support for the components is no longer available from
2097 the developer, vendor, or manufacturer.
- 2098 b. Provide options for risk mitigation or alternative sources for continued support for
2099 unsupported components if components cannot be replaced.

2100 **DISCUSSION**

2101 Support for system components includes software patches, firmware updates, replacement parts,
2102 and maintenance contracts. An example of unsupported components includes when vendors no
2103 longer provide critical software patches or product updates, which can result in opportunities for
2104 adversaries to exploit weaknesses or deficiencies in the installed components. Exceptions to
2105 replacing unsupported system components include systems that provide critical mission or
2106 business capabilities when newer technologies are unavailable or when the systems are so
2107 isolated that installing replacement components is not an option.

2108 Alternative sources for support address the need to provide continued support for system
2109 components that are no longer supported by the original manufacturers, developers, or vendors
2110 when such components remain essential to organizational mission and business functions. If
2111 necessary, organizations can establish in-house support by developing customized patches for
2112 critical software components or obtain the services of external providers who provide ongoing
2113 support for the designated unsupported components through contractual relationships. Such
2114 contractual relationships can include open-source software value-added vendors. The increased
2115 risk of using unsupported system components can be mitigated, for example, by prohibiting the
2116 connection of such components to public or uncontrolled networks or implementing other forms
2117 of isolation.

2118 **REFERENCES**

2119 Source Control: [SA-22](#)
2120 Supporting Publications: None

2121 **3.16.3. External System Services**

2122 **REQUIREMENT:** 03.16.03

- 2123 a. Require the providers of external system services used for the processing, storage, or
2124 transmission of CUI, to comply with the following security requirements: [*Assignment:*
2125 *organization-defined security requirements*].
- 2126 b. Define and document user roles and responsibilities with regard to external system services
2127 including shared responsibilities with external providers.
- 2128 c. Implement processes, methods, and techniques to monitor security requirement compliance
2129 by external service providers on an ongoing basis.

2130 **DISCUSSION**

2131 External system services are provided by external service providers. Organizations establish
2132 relationships with external service providers in a variety of ways, including through business
2133 partnerships, contracts, interagency agreements, lines of business arrangements, licensing
2134 agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks
2135 from the use of external system services remains with the organization charged with protecting

2136 CUI. Service-level agreements define the expectations of performance, describe measurable
2137 outcomes, and identify remedies, mitigations, and response requirements for instances of
2138 noncompliance. Information from external service providers regarding the specific functions,
2139 ports, protocols, and services used in the provision of such services can be useful when there is
2140 a need to understand the trade-offs involved in restricting certain functions and services or
2141 blocking certain ports and protocols. This requirement is related to [03.01.20](#).

2142 REFERENCES

2143 Source Control: [SA-09](#)
2144 Supporting Publications: SP 800-160-1 [11], SP 800-161 [33]

2145 3.17. [Supply Chain Risk Management](#)

2146 3.17.1. Supply Chain Risk Management Plan

2147 REQUIREMENT: 03.17.01

- 2148 a. Develop a plan for managing supply chain risks associated with the research, development,
2149 design, manufacturing, acquisition, delivery, integration, operations, maintenance, and
2150 disposal of the system, system components, or system services.
- 2151 b. Review and update the supply chain risk management plan periodically.
- 2152 c. Protect the supply chain risk management plan from unauthorized disclosure.

2153 DISCUSSION

2154 Dependence on the products, systems, and services from external providers and the nature of the
2155 relationships with those providers present an increasing level of risk to an organization. Threat
2156 actions that may increase security risks include unauthorized production; the insertion or use of
2157 counterfeits; tampering; theft; the insertion of malicious software, firmware, and hardware; and
2158 poor manufacturing and development practices in the supply chain. Supply chain risks can be
2159 endemic or systemic within a system, component, or service. Managing supply chain risks is a
2160 complex, multifaceted undertaking that requires a coordinated effort across an organization to
2161 build trust relationships and communicate with internal and external stakeholders.

2162 Supply chain risk management (SCRM) activities include identifying and assessing risks,
2163 determining appropriate risk response actions, developing SCRM plans to document response
2164 actions, and monitoring performance against the plans. The system-level SCRM plan is
2165 implementation-specific and provides policy implementation, requirements, constraints, and
2166 implications. It can either be stand-alone or incorporated into system security plans. The SCRM
2167 plan addresses the management, implementation, and monitoring of SCRM controls and the
2168 development or sustainment of systems across the system development life cycle to support
2169 mission and business functions. Because supply chains can differ significantly across and within
2170 organizations, SCRM plans are tailored to individual program, organizational, and operational
2171 contexts.

2172 REFERENCES

2173 Source Control: [SR-02](#)
2174 Supporting Publications: SP 800-30 [55], SP 800-39 [60], SP 800-160-1 [11], SP 800-181 [34]

2175 **3.17.2. Acquisition Strategies, Tools, and Methods**

2176 **REQUIREMENT:** 03.17.02

2177 Develop and implement acquisition strategies, contract tools, and procurement methods to
2178 identify, protect against, and mitigate supply chain risks.

2179 **DISCUSSION**

2180 The acquisition process provides an important vehicle for protecting the supply chain. There are
2181 many useful tools and techniques available, including obscuring the end use of a system or
2182 system component, using blind or filtered buys, requiring tamper-evident packaging, or using
2183 trusted or controlled distribution. The results from a supply chain risk assessment can inform
2184 the strategies, tools, and methods that are most applicable to the situation. Tools and techniques
2185 may provide protections against unauthorized production, theft, tampering, the insertion of
2186 counterfeits, the insertion of malicious software or backdoors, and poor development practices
2187 throughout the system life cycle.

2188 Organizations also consider providing incentives for suppliers to implement controls, promote
2189 transparency in their processes and security practices, provide contract language that addresses
2190 the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy
2191 suppliers. Organizations consider providing training, education, and awareness programs for
2192 personnel regarding supply chain risk, available mitigation strategies, and when the programs
2193 should be employed. Methods for reviewing and protecting development plans, documentation,
2194 and evidence are commensurate with the security requirements of the organization. Contracts
2195 may specify documentation protection requirements.

2196 **REFERENCES**

2197 Source Control: [SR-05](#)
2198 Supporting Publications: SP 800-30 [55], SP 800-161 [33]

2199 **3.17.3. Supply Chain Requirements and Processes**

2200 **REQUIREMENT:** 03.17.03

- 2201 a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply
2202 chain elements and processes.
- 2203 b. Enforce the following security requirements to protect against supply chain risks to the
2204 system, system components, or system services and to limit the harm or consequences
2205 from supply chain-related events: [*Assignment: organization-defined security requirements*].

2206 **DISCUSSION**

2207 Supply chain elements include organizations, entities, or tools that are employed for the
2208 research, development, design, manufacturing, acquisition, delivery, integration, operations and
2209 maintenance, and disposal of systems and system components. Supply chain processes include
2210 hardware, software, firmware, and systems development processes; shipping and handling
2211 procedures; personnel and physical security programs; configuration management tools,
2212 techniques, and measures to maintain provenance; or other programs, processes, or procedures
2213 associated with the development, acquisition, maintenance, and disposal of systems and system
2214 components. Supply chain elements and processes may be provided by organizations, system
2215 integrators, or external providers. Weaknesses or deficiencies in supply chain elements or

2216 processes represent potential vulnerabilities that can be exploited by adversaries to harm the
2217 organization and affect its ability to carry out its core missions or business functions.

2218 **REFERENCES**

2219 Source Control: [SR-03](#)

2220 Supporting Publications: SP 800-30 [55], SP 800-161 [33]

2221 **References**

- 2222 [1] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House,
2223 Washington, DC), DCPD-201000942, November 4, 2010. Available at
2224 <https://www.govinfo.gov/app/details/DCPD-201000942>
- 2225 [2] Executive Order 13526 (2009) Classified National Security Information. (The White House,
2226 Washington, DC), DCPD-200901022, December 29, 2009. Available at
2227 <https://www.govinfo.gov/app/details/DCPD-200901022>
- 2228 [3] Atomic Energy Act (P.L. 83-703), August 1954. Available at
2229 <https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919>
- 2230 [4] National Archives and Records Administration (2019) Controlled Unclassified Information
2231 (CUI) Registry. Available at <https://www.archives.gov/cui>
- 2232 [5] 32 CFR Part 2002 (2016), Controlled Unclassified Information (CUI), September 2016.
2233 Available at <https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018->
2234 [title32-vol6-part2002.pdf](https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf)
- 2235 [6] National Institute of Standards and Technology (2004) Standards for Security
2236 Categorization of Federal Information and Information Systems. (U.S. Department of
2237 Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS)
2238 199. <https://doi.org/10.6028/NIST.FIPS.199>
- 2239 [7] National Institute of Standards and Technology (2006) Minimum Security Requirements for
2240 Federal Information and Information Systems. (U.S. Department of Commerce,
2241 Washington, DC), Federal Information Processing Standards Publication (FIPS) 200.
2242 <https://doi.org/10.6028/NIST.FIPS.200>
- 2243 [8] Joint Task Force (2020) Security and Privacy Controls for Information Systems and
2244 Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2245 Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020.
2246 <https://doi.org/10.6028/NIST.SP.800-53r5>
- 2247 [9] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available
2248 at <https://www.govinfo.gov/app/details/PLAW-113publ283>
- 2249 [10] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-
2250 Resilient Systems: A Systems Security Engineering Approach. (National Institute of
2251 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160,
2252 Vol. 2, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- 2253 [11] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems.
2254 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2255 Publication (SP) 800-160, Vol. 1, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-160v1r1>
- 2256 [12] Joint Task Force (2020) Control Baselines for Systems and Organizations. (National
2257 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2258 800-53B, Includes updates as of December 10, 2020. <https://doi.org/10.6028/NIST.SP.800->
2259 [53B](https://doi.org/10.6028/NIST.SP.800-53B)
- 2260 [13] Office of Management and Budget Circular A-130, Managing Information as a Strategic
2261 Resource, July 2016. Available at <https://www.whitehouse.gov/wp->
2262 [content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

- 2263 [14] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and
2264 Bring Your Own Device (BYOD) Security. (National Institute of Standards and
2265 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2.
2266 <https://doi.org/10.6028/NIST.SP.800-46r2>
- 2267 [15] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National
2268 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2269 800-57 Part 1, Rev. 5. <https://doi.org/10.6028/NIST.SP.800-57pt1r5>
- 2270 [16] Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best
2271 Practices for Key Management Organizations. (National Institute of Standards and
2272 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1.
2273 <https://doi.org/10.6028/NIST.SP.800-57pt2r1>
- 2274 [17] Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-
2275 Specific Key Management Guidance. (National Institute of Standards and Technology,
2276 Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1.
2277 <https://doi.org/10.6028/NIST.SP.800-57pt3r1>
- 2278 [18] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs.
2279 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2280 Publication (SP) 800-77, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-77r1>
- 2281 [19] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National
2282 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2283 800-113. <https://doi.org/10.6028/NIST.SP.800-113>
- 2284 [20] Souppaya MP, Scarfone KA (2016) User’s Guide to Telework and Bring Your Own Device
2285 (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD),
2286 NIST Special Publication (SP) 800-114, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-114r1>
- 2287 [21] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide
2288 to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD),
2289 NIST Special Publication (SP) 800-121, Rev. 2, Includes updates as of January 19, 2022.
2290 <https://doi.org/10.6028/NIST.SP.800-121r2-upd1>
- 2291 [22] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014)
2292 Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National
2293 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2294 800-162, Includes updates as of August 2, 2019. <https://doi.org/10.6028/NIST.SP.800-162>
- 2295 [23] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based
2296 Access Control (ABAC) Standards for Data Service Applications: Extensible Access
2297 Control Markup Language (XACML) and Next Generation Access Control (NGAC).
2298 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2299 Publication (SP) 800-178. <https://doi.org/10.6028/NIST.SP.800-178>
- 2300 [24] Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control
2301 Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2302 Special Publication (SP) 800-192. <https://doi.org/10.6028/NIST.SP.800-192>
- 2303 [25] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics.
2304 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or
2305 Internal Report (IR) 7874. <https://doi.org/10.6028/NIST.IR.7874>

- 2306 [26] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and
2307 Automated Access Management Using Secure Shell (SSH). (National Institute of Standards
2308 and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966.
2309 <https://doi.org/10.6028/NIST.IR.7966>
- 2310 [27] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of
2311 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3,
2312 Includes updates as of March 2, 2020. <https://doi.org/10.6028/NIST.SP.800-63-3>
- 2313 [28] Howell G, Franklin JM, Sritapan V, Souppaya M, Scarfone K (2023) Guidelines for
2314 Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards
2315 and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 2.
2316 <https://doi.org/10.6028/NIST.SP.800-124r2>
- 2317 [29] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems
2318 (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2319 Publication (SP) 800-94. <https://doi.org/10.6028/NIST.SP.800-94>
- 2320 [30] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security
2321 Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology,
2322 Gaithersburg, MD), NIST Special Publication (SP) 800-97.
2323 <https://doi.org/10.6028/NIST.SP.800-97>
- 2324 [31] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device
2325 (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD),
2326 NIST Special Publication (SP) 800-114, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-114r1>
- 2327 [32] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and
2328 Training Program. (National Institute of Standards and Technology, Gaithersburg, MD),
2329 NIST Special Publication (SP) 800-50. <https://doi.org/10.6028/NIST.SP.800-50>
- 2330 [33] Boyens JM, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity
2331 Supply Chain Risk Management Practices for Systems and Organizations. (National
2332 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2333 800-161, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-161r1>
- 2334 [34] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for
2335 Cybersecurity (NICE Framework). (National Institute of Standards and Technology,
2336 Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1.
2337 <https://doi.org/10.6028/NIST.SP.800-181r1>
- 2338 [35] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National
2339 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2340 800-92. <https://doi.org/10.6028/NIST.SP.800-92>
- 2341 [36] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques
2342 into Incident Response. (National Institute of Standards and Technology, Gaithersburg,
2343 MD), NIST Special Publication (SP) 800-86. <https://doi.org/10.6028/NIST.SP.800-86>
- 2344 [37] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National
2345 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2346 800-101, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-101r1>
- 2347 [38] National Institute of Standards and Technology (2019) Security Requirements for
2348 Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal
2349 Information Processing Standards Publication (FIPS) 140-3.
2350 <https://doi.org/10.6028/NIST.FIPS.140-3>

- 2351 [39] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S.
2352 Department of Commerce, Washington, D.C.), Federal Information Processing Standards
2353 Publication (FIPS) 180-4. <https://doi.org/10.6028/NIST.FIPS.180-4>
- 2354 [40] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based
2355 Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington,
2356 D.C.), Federal Information Processing Standards Publication (FIPS) 202.
2357 <https://doi.org/10.6028/NIST.FIPS.202>
- 2358 [41] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused
2359 Configuration Management of Information Systems. (National Institute of Standards and
2360 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates
2361 as of October 10, 2019. <https://doi.org/10.6028/NIST.SP.800-128>
- 2362 [42] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control
2363 Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and
2364 Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2.
2365 <https://doi.org/10.6028/NIST.IR.8011-2>
- 2366 [43] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control
2367 Assessments: Volume 3: Software Asset Management. (National Institute of Standards and
2368 Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3.
2369 <https://doi.org/10.6028/NIST.IR.8011-3>
- 2370 [44] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for
2371 IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards
2372 and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4.
2373 <https://doi.org/10.6028/NIST.SP.800-70r4>
- 2374 [45] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical
2375 Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3.
2376 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2377 Publication (SP) 800-126, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-126r3>
- 2378 [46] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting.
2379 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2380 Publication (SP) 800-167. <https://doi.org/10.6028/NIST.SP.800-167>
- 2381 [47] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident
2382 Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2383 Special Publication (SP) 800-61, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-61r2>
- 2384 [48] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training,
2385 and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and
2386 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84.
2387 <https://doi.org/10.6028/NIST.SP.800-84>
- 2388 [49] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA,
2389 Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal
2390 Information Systems and Organizations. (National Institute of Standards and Technology,
2391 Gaithersburg, MD), NIST Special Publication (SP) 800-137.
2392 <https://doi.org/10.6028/NIST.SP.800-137>
- 2393 [50] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media
2394 Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2395 Special Publication (SP) 800-88, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-88r1>

- 2396 [51] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies
2397 for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD),
2398 NIST Special Publication (SP) 800-111. <https://doi.org/10.6028/NIST.SP.800-111>
- 2399 [52] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning
2400 Guide for Federal Information Systems. (National Institute of Standards and Technology,
2401 Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of
2402 November 11, 2010. <https://doi.org/10.6028/NIST.SP.800-34r1>
- 2403 [53] Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing
2404 Cryptographic Key Management Systems. (National Institute of Standards and Technology,
2405 Gaithersburg, MD), NIST Special Publication (SP) 800-130.
2406 <https://doi.org/10.6028/NIST.SP.800-130>
- 2407 [54] Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key
2408 Management Systems (CKMS). (National Institute of Standards and Technology,
2409 Gaithersburg, MD), NIST Special Publication (SP) 800-152.
2410 <https://doi.org/10.6028/NIST.SP.800-152>
- 2411 [55] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments.
2412 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2413 Publication (SP) 800-30, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- 2414 [56] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning:
2415 Preventive Maintenance for Technology. (National Institute of Standards and Technology,
2416 Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4.
2417 <https://doi.org/10.6028/NIST.SP.800-40r4>
- 2418 [57] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls
2419 in Information Systems and Organizations. (National Institute of Standards and Technology,
2420 Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5.
2421 <https://doi.org/10.6028/NIST.SP.800-53Ar5>
- 2422 [58] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information
2423 Security Testing and Assessment. (National Institute of Standards and Technology,
2424 Gaithersburg, MD), NIST Special Publication (SP) 800-115.
2425 <https://doi.org/10.6028/NIST.SP.800-115>
- 2426 [59] Joint Task Force (2018) Risk Management Framework for Information Systems and
2427 Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute
2428 of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37,
2429 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- 2430 [60] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:
2431 Organization, Mission, and Information System View. (National Institute of Standards and
2432 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
2433 <https://doi.org/10.6028/NIST.SP.800-39>
- 2434 [61] Nieves M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security.
2435 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2436 Publication (SP) 800-12, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-12r1>
- 2437 [62] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers.
2438 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2439 Publication (SP) 800-100, Includes updates as of March 7, 2007.
2440 <https://doi.org/10.6028/NIST.SP.800-100>

- 2441 [63] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal
2442 Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD),
2443 NIST Special Publication (SP) 800-18, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-18r1>
- 2444 [64] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National
2445 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2446 800-41, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-41r1>
- 2447 [65] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM)
2448 Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2449 Special Publication (SP) 800-125B. <https://doi.org/10.6028/NIST.SP.800-125B>
- 2450 [66] Rose S, Borchert O, Mitchell S, Connelly S (2017) Zero Trust Architecture. (National
2451 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2452 800-207. <https://doi.org/10.6028/NIST.SP.800-207>
- 2453 [67] Sriram K, Montgomery D (2019) Resilient Interdomain Traffic Exchange: BGP Security
2454 and DDoS Mitigation. (National Institute of Standards and Technology, Gaithersburg, MD),
2455 NIST Special Publication (SP) 800-189. <https://doi.org/10.6028/NIST.SP.800-189>
- 2456 [68] National Institute of Standards and Technology (2001) Advanced Encryption Standard
2457 (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing
2458 Standards Publication (FIPS) 197, updated May 9, 2023.
2459 <https://doi.org/10.6028/NIST.FIPS.197-upd1>
- 2460 [69] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of
2461 Transport Layer Security (TLS) Implementations. (National Institute of Standards and
2462 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2.
2463 <https://doi.org/10.6028/NIST.SP.800-52r2>
- 2464 [70] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email.
2465 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2466 Publication (SP) 800-177, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-177r1>
- 2467 [71] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile
2468 Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2469 Publication (SP) 800-28, Version 2. <https://doi.org/10.6028/NIST.SP.800-28ver2>
- 2470 [72] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National
2471 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2472 800-95. <https://doi.org/10.6028/NIST.SP.800-95>
- 2473 [73] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-
2474 Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National
2475 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2476 800-56A, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>
- 2477 [74] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation
2478 for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National
2479 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
2480 800-56B, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-56Br2>
- 2481 [75] Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-
2482 Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg,
2483 MD), NIST Special Publication (SP) 800-56C, Rev. 2.
2484 <https://doi.org/10.6028/NIST.SP.800-56Cr2>

- 2485 [76] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for
2486 Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD),
2487 NIST Special Publication (SP) 800-83, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-83r1>
- 2488 [77] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail
2489 Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2490 Special Publication (SP) 800-45, Version 2. <https://doi.org/10.6028/NIST.SP.800-45ver2>
- 2491 [78] Committee on National Security Systems (2022) Committee on National Security Systems
2492 (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS
2493 Instruction 4009. Available at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- 2494 [79] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. Available at
2495 [https://www.govinfo.gov/app/details/USCODE-2017-](https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-)
2496 [chap35-subchapII-sec3552](https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-)
- 2497 [80] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards.
2498 2017 ed. Available at <https://www.govinfo.gov/app/details/USCODE-2017->
2499 [title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331](https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331)
- 2500 [81] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at
2501 <https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44->
2502 [chap35-subchapI-sec3502](https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-)
- 2503 [82] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide.
2504 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2505 Publication (SP) 800-81-2. <https://doi.org/10.6028/NIST.SP.800-81-2>
- 2506 [83] Dempsey K, Pillitteri V, Regenscheid A (2021) Managing the Security of Information
2507 Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2508 Special Publication (SP) 800-47, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-47r1>

2509 **Appendix A. Acronyms**

2510 **CFR**

2511 Code of Federal Regulations

2512 **CISA**

2513 Cybersecurity and Infrastructure Security Agency

2514 **CUI**

2515 Controlled Unclassified Information

2516 **CVE**

2517 Common Vulnerabilities and Exposures

2518 **CVSS**

2519 Common Vulnerabilities Scoring System

2520 **CWE**

2521 Common Weakness Enumeration

2522 **DMZ**

2523 Demilitarized Zone

2524 **EAP**

2525 Extensible Authentication Protocol

2526 **EO**

2527 Executive Order

2528 **FIPS**

2529 Federal Information Processing Standards

2530 **FISMA**

2531 Federal Information Security Modernization Act

2532 **FTP**

2533 File Transfer Protocol

2534 **GMT**

2535 Greenwich Mean Time

2536 **IEEE**

2537 Institute of Electrical and Electronics Engineers

2538 **IIoT**

2539 Industrial Internet of Things

2540 **IoT**

2541 Internet of Things

2542 **ISOO**

2543 Information Security Oversight Office

2544 **IT**

2545 Information Technology

2546	LSI
2547	Large-Scale Integration
2548	MAC
2549	Media Access Control
2550	NARA
2551	National Archives and Records Administration
2552	NVD
2553	National Vulnerabilities Database
2554	ODP
2555	Organization-Defined Parameter
2556	OMB
2557	Office of Management and Budget
2558	OT
2559	Operational Technology
2560	PII
2561	Personally Identifiable Information
2562	PIN
2563	Personal Identification Number
2564	PROM
2565	Programmable Read-Only Memory
2566	ROM
2567	Read-Only Memory
2568	SCAP
2569	Security Content Automation Protocol
2570	SCRM
2571	Supply Chain Risk Management
2572	SP
2573	Special Publication
2574	TCP/IP
2575	Transmission Control Protocol/Internet Protocol
2576	TLS
2577	Transport Layer Security
2578	UTC
2579	Coordinated Universal Time

2580 **Appendix B. Glossary**

2581 Appendix B provides definitions for the terminology used in NIST SP 800-171. The definitions
2582 are consistent with the definitions contained in the National Information Assurance Glossary [78]
2583 unless otherwise noted.

2584 **agency**

2585 Any executive agency or department, military department, Federal Government corporation, Federal Government-
2586 controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any
2587 independent regulatory agency. [13]

2588 **assessment**

2589 See *security control assessment*.

2590 **assessor**

2591 See *security control assessor*.

2592 **audit log**

2593 A chronological record of system activities, including records of system accesses and operations performed in a
2594 given period.

2595 **audit record**

2596 An individual entry in an audit log related to an audited event.

2597 **authentication**

2598 Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a
2599 system. Adapted from [7].

2600 **availability**

2601 Ensuring timely and reliable access to and use of information. [79]

2602 **advanced persistent threat**

2603 An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create
2604 opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and
2605 deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the
2606 targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a
2607 mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced
2608 persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it;
2609 and is determined to maintain the level of interaction needed to execute its objectives. [60]

2610 **authenticator**

2611 Something the claimant possesses and controls (typically a cryptographic module or password) that is used to
2612 authenticate the claimant's identity. This was previously referred to as a token.

2613 **baseline configuration**

2614 A documented set of specifications for a system or a configuration item within a system that has been formally
2615 reviewed and agreed upon at a given point in time, and that can only be changed through change control procedures.

2616 **common secure configuration**

2617 Recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific
2618 information technology platforms/products and instructions for configuring those system components to meet
2619 operational requirements. These benchmarks are also referred to as security configuration checklists, lockdown and
2620 hardening guides, security reference guides, and security technical implementation guides.

- 2621 **confidentiality**
2622 Preserving authorized restrictions on information access and disclosure, including means for protecting personal
2623 privacy and proprietary information. [79]
- 2624 **configuration management**
2625 A collection of activities focused on establishing and maintaining the integrity of information technology products
2626 and systems through the control of processes for initializing, changing, and monitoring the configurations of those
2627 products and systems throughout the system development life cycle.
- 2628 **configuration settings**
2629 The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or
2630 functionality of the system.
- 2631 **controlled area**
2632 Any area or space for which the organization has confidence that the physical and procedural protections provided
2633 are sufficient to meet the requirements established for protecting the information or system.
- 2634 **controlled unclassified information**
2635 Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls,
2636 excluding information that is classified under Executive Order 13526, Classified National Security Information,
2637 December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [1]
- 2638 **CUI Executive Agent**
2639 The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI
2640 Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this
2641 authority to the Director of the Information Security Oversight Office (ISOO). [5]
- 2642 **CUI program**
2643 The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the
2644 rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI
2645 Registry. [5]
- 2646 **CUI registry**
2647 The online repository for all information, guidance, policy, and requirements on handling CUI, including everything
2648 issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry
2649 identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls,
2650 establishes markings, and includes guidance on handling procedures. [5]
- 2651 **cyber-physical systems**
2652 Interacting digital, analog, physical, and human components engineered for function through integrated physics and
2653 logic.
- 2654 **executive agency**
2655 An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an
2656 independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully
2657 subject to the provisions of 31 U.S.C. Chapter 91.
- 2658 **external system (or component)**
2659 A system or component of a system that is outside of the authorization boundary established by the organization and
2660 for which the organization typically has no direct control over the application of required security controls or the
2661 assessment of security control effectiveness.

- 2662 **external system service**
2663 A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a
2664 service that is used by but not a part of the organizational system) and for which the organization typically has no
2665 direct control over the application of required security controls or the assessment of security control effectiveness.
- 2666 **external network**
2667 A network not controlled by the organization.
- 2668 **facility**
2669 One or more physical locations containing systems or system components that process, store, or transmit
2670 information.
- 2671 **federal agency**
2672 See *executive agency*.
- 2673 **federal information system**
2674 An information system used or operated by an executive agency, by a contractor of an executive agency, or by
2675 another organization on behalf of an executive agency. [80]
- 2676 **FIPS-validated cryptography**
2677 A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet the
2678 requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the
2679 cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed
2680 validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-approved cryptography*.
- 2681 **firmware**
2682 Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-
2683 only memory (PROM) – such that the programs and data cannot be dynamically written or modified during
2684 execution of the programs. See *hardware* and *software*. [78]
- 2685 **hardware**
2686 The material physical components of a system. See *software* and *firmware*. [78]
- 2687 **identifier**
2688 Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples
2689 of identifiers.
- 2690 A unique label used by a system to indicate a specific entity, object, or group.
- 2691 **impact**
2692 With respect to security, the effect on organizational operations, organizational assets, individuals, other
2693 organizations, or the Nation (including the national security interests of the United States) of a loss of
2694 confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that
2695 individuals could experience when an information system processes their PII.
- 2696 **impact value**
2697 The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or
2698 availability of information expressed as a value of low, moderate or high. [6]
- 2699 **incident**
2700 An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or
2701 availability of information or an information system; or constitutes a violation or imminent threat of violation of
2702 law, security policies, security procedures, or acceptable use policies. [79]

- 2703 **information**
2704 Any communication or representation of knowledge such as facts, data, or opinions in any medium or form,
2705 including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [13]
- 2706 **information flow control**
2707 Procedure to ensure that information transfers within a system do not violate the security policy.
- 2708 **information resources**
2709 Information and related resources, such as personnel, equipment, funds, and information technology. [81]
- 2710 **information security**
2711 The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or
2712 destruction in order to provide confidentiality, integrity, and availability. [79]
- 2713 **information system**
2714 A discrete set of information resources organized for the collection, processing, maintenance, use, sharing,
2715 dissemination, or disposition of information. [81]
- 2716 **information technology**
2717 Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic
2718 acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching,
2719 interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such
2720 services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that
2721 requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product.
2722 Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and
2723 storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the
2724 central processing unit of a computer, software, firmware and similar procedures, services (including cloud
2725 computing and help-desk services or other professional services which support any point of the life cycle of the
2726 equipment or service), and related resources. Information technology does not include any equipment that is
2727 acquired by a contractor incidental to a contract which does not require its use. [13]
- 2728 **insider threat**
2729 The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of
2730 the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized
2731 disclosure, or through the loss or degradation of departmental resources or capabilities.
- 2732 **integrity**
2733 Guarding against improper information modification or destruction and includes ensuring information non-
2734 repudiation and authenticity. [79]
- 2735 **internal network**
2736 A network in which the establishment, maintenance, and provisioning of security controls are under the direct
2737 control of organizational employees or contractors or in which the cryptographic encapsulation or similar security
2738 technology implemented between organization-controlled endpoints provides the same effect (with regard to
2739 confidentiality and integrity). An internal network is typically organization-owned yet may be organization-
2740 controlled while not being organization-owned.
- 2741 **least privilege**
2742 The principle that a security architecture is designed so that each entity is granted the minimum system
2743 authorizations and resources needed to perform its function.
- 2744 **malicious code**
2745 Software or firmware intended to perform an unauthorized process that will have an adverse impact on the
2746 confidentiality, integrity, or availability of a system. Examples of malicious code include viruses, worms, Trojan
2747 horses, spyware, some forms of adware, or other code-based entities that infect a host.

- 2748 **media**
2749 Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks,
2750 Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which
2751 information is recorded, stored, or printed within a system. [7]
- 2752 **mobile code**
2753 Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed
2754 on a local system without explicit installation or execution by the recipient.
- 2755 **mobile device**
2756 A portable computing device that has a small form factor such that it can easily be carried by a single individual; is
2757 designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local,
2758 non-removable, or removable data storage; and includes a self-contained power source. Mobile devices may also
2759 include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in
2760 features that synchronize local data with remote locations. Examples include smartphones, tablets, and e-readers.
- 2761 **multi-factor authentication**
2762 Authentication using two or more different factors to achieve authentication. Factors include something you know
2763 (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are
2764 (e.g., biometric). See *authenticator*.
- 2765 **network**
2766 A system implemented with a collection of interconnected components. Such components may include routers,
2767 hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
- 2768 **network access**
2769 Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local
2770 area network, wide area network, the internet).
- 2771 **nonfederal organization**
2772 An entity that owns, operates, or maintains a nonfederal system.
- 2773 **nonfederal system**
2774 A system that does not meet the criteria for a federal system.
- 2775 **nonlocal maintenance**
2776 Maintenance activities conducted by individuals communicating through an external network (e.g., the internet) or
2777 an internal network.
- 2778 **NSA-approved cryptography**
2779 Cryptography that consists of an approved algorithm, an implementation that has been approved for the protection of
2780 classified information and/or controlled unclassified information in a specific environment, and a supporting key
2781 management infrastructure. [8]
- 2782 **on behalf of (an agency)**
2783 A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains
2784 or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those
2785 activities are not incidental to providing a service or product to the government. [5]
- 2786 **organization**
2787 An entity of any size, complexity, or positioning within an organizational structure. Adapted from [7]
- 2788 **organization-defined parameter**
2789 The variable part of a security requirement that is instantiated by an organization during the tailoring process by
2790 assigning an organization-defined value as part of the requirement. Adapted from [8].

- 2791 **overlay**
2792 A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting
2793 information employed during the tailoring process, that is intended to complement (and further refine) security
2794 control baselines. The overlay specification may be more stringent or less stringent than the original security control
2795 baseline specification and can be applied to multiple information systems. [13]
- 2796 **personnel security**
2797 The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties
2798 and responsibilities requiring trustworthiness. [8]
- 2799 **portable storage device**
2800 A system component that can be inserted into and removed from a system and that is used to store information or
2801 data (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical,
2802 or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives,
2803 flash memory cards/drives that contain nonvolatile memory).
- 2804 **potential impact**
2805 The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS
2806 Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic
2807 adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals. [6]
- 2808 **privileged account**
2809 A system account with the authorizations of a privileged user.
- 2810 **privileged user**
2811 A user who is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not
2812 authorized to perform.
- 2813 **records**
2814 The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms,
2815 reports, test results) that serve as a basis for verifying that the organization and the system are performing as
2816 intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a
2817 program and that contain a complete set of information on particular items).
- 2818 **remote access**
2819 Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an
2820 external network (e.g., the internet). Remote access methods include dial-up, broadband, and wireless.
- 2821 **remote maintenance**
2822 Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).
- 2823 **replay resistant**
2824 Protection against the capture of transmitted authentication or access control information and its subsequent
2825 retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
- 2826 **risk**
2827 A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a
2828 function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
2829 (ii) the likelihood of occurrence. [13]
- 2830 **risk assessment**
2831 The process of identifying risks to organizational operations (including mission, functions, image, reputation),
2832 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. [55]

- 2833 **sanitization**
2834 Actions taken to render data written on media unrecoverable by ordinary and — for some forms of sanitization —
2835 extraordinary means.
- 2836 A process to remove information from media such that data recovery is not possible, including the removal of all
2837 classified labels, markings, and activity logs.
- 2838 **security**
2839 A condition that results from the establishment and maintenance of protective measures that enable an organization
2840 to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures
2841 may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should
2842 form part of the organization’s risk management approach. [78]
- 2843 **security assessment**
2844 See *security control assessment*.
- 2845 **security control**
2846 The safeguards or countermeasures prescribed for an information system or an organization to protect the
2847 confidentiality, integrity, and availability of the system and its information. [13]
- 2848 **security control assessment**
2849 The testing or evaluation of security controls to determine the extent to which the controls are implemented
2850 correctly, operating as intended, and producing the desired outcome with respect to meeting the security
2851 requirements for an information system or organization. [13]
- 2852 **security domain**
2853 A domain that implements a security policy and is administered by a single authority. Adapted from [78]
- 2854 **security functions**
2855 The hardware, software, or firmware of the system responsible for enforcing the system security policy and
2856 supporting the isolation of code and data on which the protection is based.
- 2857 **security requirement**
2858 A requirement levied on a system or an organization that is derived from applicable laws, Executive Orders,
2859 directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality,
2860 integrity, and availability of information that is being processed, stored, or transmitted. Adapted from [7] and [8].
- 2861 **split tunneling**
2862 The process of allowing a remote user or device to establish a non-remote connection with a system and
2863 simultaneously communicate via some other connection to a resource in an external network. This method of
2864 network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing
2865 uncontrolled networks.
- 2866 **system**
2867 See *information system*.
- 2868 **system component**
2869 A discrete identifiable information technology asset that represents a building block of a system and may include
2870 hardware, software, and firmware. [41]
- 2871 **system security plan**
2872 A document that describes how an organization meets or plans to meet the security requirements for a system. In
2873 particular, the system security plan describes the system boundary, the environment in which the system operates,
2874 how the security requirements are implemented, and the relationships with or connections to other systems.

2875 **system service**

2876 A capability provided by a system that facilitates information processing, storage, or transmission.

2877 **threat**

2878 Any circumstance or event with the potential to adversely impact organizational operations, organizational assets,
2879 individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure,
2880 modification of information, and/or denial of service. [55]

2881 **system user**

2882 An individual or (system) process acting on behalf of an individual that is authorized to access a system.

2883 **Appendix C. Tailoring Criteria**

2884 This appendix describes the security control tailoring criteria used to develop the CUI security
 2885 requirements. [Table 2](#) lists the available tailoring options and the shorthand tailoring symbols.
 2886 [Table 3](#) through [Table 22](#) specify the tailoring actions applied to the controls in the NIST SP
 2887 800-53 moderate baseline [12] to obtain the security requirements in [Section 3](#). The controls and
 2888 control enhancements are hyperlinked to the NIST [Cybersecurity and Privacy Reference Tool](#),
 2889 which provides online access to the specific control language and supplemental materials in
 2890 NIST SP 800-53.

2891 **Table 2. Security control tailoring criteria**

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

2892

2893 **Table 3. [Access Control \(AC\)](#)**

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

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

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

2894

2895

Table 4. [Awareness and Training \(AT\)](#)

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

2896

2897

Table 5. [Audit and Accountability \(AU\)](#)

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

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

2898

2899

Table 6. [Assessment, Authorization, and Monitoring \(CA\)](#)

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

2900

2901

Table 7. [Configuration Management \(CM\)](#)

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

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

2902

2903

Table 8. [Contingency Planning \(CP\)](#)

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

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

2904

Table 9. [Identification and Authentication \(IA\)](#)

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

2905

2906

2907

Table 10. [Incident Response \(IR\)](#)

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

2908

2909

Table 11. [Maintenance \(MA\)](#)

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

2910

2911

Table 12. [Media Protection \(MP\)](#)

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

2912

Table 13. [Physical and Environmental Protection \(PE\)](#)

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

2913

2914

Table 14. [Planning \(PL\)](#)

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

2915

2916

Table 15. [Program Management \(PM\)](#)

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

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

2917

2918

Table 16. [Personnel Security \(PS\)](#)

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

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

2919

2920

Table 17. [PII Processing and Transparency \(PT\)](#)

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

2921

2922

Table 18. [Risk Assessment \(RA\)](#)

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

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

2923

2924

Table 19. [System and Services Acquisition \(SA\)](#)

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

2925

2926

Table 20. [System and Communications Protection \(SC\)](#)

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

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

2927

2928

Table 21. [System and Information Integrity \(SI\)](#)

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

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

2929

2930

Table 22. [Supply Chain Risk Management \(SR\)](#)

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

2931

2932 **Appendix D. Change Log**

2933 This publication incorporates the following changes from the original edition (February 2020;
2934 updated January 28, 2021):

- 2935 • Streamlined introductory information in [Section 1](#) and [Section 2](#) to improve clarity and
2936 understanding
- 2937 • Modified the security requirements and families in [Section 3](#) to reflect the security
2938 controls in the NIST SP 800-53B [12] moderate baseline and the tailoring actions in
2939 [Appendix C](#)
- 2940 • Eliminated the distinction between basic and derived security requirements
- 2941 • Increased the specificity of security requirements to remove ambiguity, improve the
2942 effectiveness of implementation, and clarify the scope of assessments
- 2943 • Introduced organization-defined parameters (ODPs) in selected security requirements to
2944 increase flexibility and help organizations better manage risk
- 2945 • Grouped security requirements, where possible, to improve understanding and the
2946 efficiency of implementations and assessments
- 2947 • Removed outdated and redundant security requirements
- 2948 • Added new security requirements
- 2949 • Added titles to security requirements
- 2950 • Restructured and streamlined the discussion sections for security requirements
- 2951 • Introduced new tailoring categories: *Other Related Controls (ORC)* and *Not Applicable*
2952 (*N/A*)
- 2953 • Recategorized selected controls in the NIST SP 800-53B moderate baseline (using the
2954 tailoring criteria in [Appendix C](#))
- 2955 • Revised the security requirements for consistency with the security control language in
2956 NIST SP 800-53
- 2957 • Revised the structure of the [References](#), [Acronyms](#), and [Glossary](#) sections for greater
2958 clarity and ease of use
- 2959 • Revised the tailoring tables in [Appendix C](#) for consistency with the changes to the
2960 security requirements

2961 [Table 23](#) shows the changes incorporated into this publication. Errata updates can include
2962 corrections, clarifications, or other minor changes in the publication that are either *editorial* or
2963 *substantive* in nature. Any potential updates to this document that are not yet published in an
2964 errata update or a formal revision, including additional issues and potential corrections, will be
2965 posted as they are identified. See the publication details for this report. The current release of this
2966 publication does not include any errata updates.

