Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-171 Rev. 1
Title:	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Publication Date(s):	December 2016 (including updates as of November 28, 2017)
Withdrawal Date:	February 20, 2018
Withdrawal Note:	SP 800-171 Rev. 1 (11/28/17 update) is superseded in its entirety by the publication of SP 800-171 Rev. 1 (2/20/18 update).

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	NIST Special Publication 800-171 Rev. 1
Title:	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Author(s):	Ron Ross; Kelley Dempsey; Patrick Viscuso; Mark Riddle; Gary Guissanie
Publication Date(s):	December 2016 (updated 2/20/2018)
URL/DOI:	https://doi.org/10.6028/NIST.SP.800-171r1

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Laboratory)
Latest revision of the attached publication:	SP 800-171 Rev. 1
Related information:	https://csrc.nist.gov https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
Withdrawal announcement (link):	N/A

Date updated: February 20, 2018

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

NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

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

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

NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Department of Defense

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

December 2016
INCLUDES UPDATES AS OF 11-28-2017

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST to further 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.

National Institute of Standards and Technology Special Publication 800-171
Natl. Inst. Stand. Technol. Spec. Publ. 800-171, **81 pages** (December 2016)

CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by 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, practices, 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 draft publications during the designated public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at **http://csrc.nist.gov/publications**.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic Mail: **sec-cert@nist.gov**

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

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 (IT). 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 systems security and its collaborative activities with industry, government, and academic organizations.

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 assigned missions and business operations. This publication provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Keywords

Contractor Systems; Controlled Unclassified Information; CUI Registry; Derived Security Requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; Nonfederal Systems; Security Assessment; Security Control; Security Requirement.

Acknowledgements

The authors gratefully acknowledge and appreciate the contributions from Carol Bales, Matt Barrett, Jon Boyens, Devin Casey, Chris Enloe, Jim Foti, Rob Glenn, Rich Graubart, Vicki Michetti, Victoria Pillitteri, Pat O'Reilly, Karen Quigg, Mary Thomas, Matt Scholl, Murugiah Souppaya, and Pat Toth, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb administrative and technical editing support.

CAUTIONARY NOTE

The Federal Information Security Modernization Act (FISMA) of 2014 requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. This publication focuses on protecting the *confidentiality* of Controlled Unclassified Information (CUI) in *nonfederal* systems and organizations, and recommends specific security requirements to achieve that objective. It does not change the information security requirements set forth in FISMA, nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute, the policies established by OMB, and the supporting security standards and guidelines developed by NIST.

The requirements recommended for use in this publication are derived from FIPS Publication 200 and the moderate security control baseline in NIST Special Publication 800-53 and are based on the CUI regulation (32 CFR Part 2002, *Controlled Unclassified Information*). The requirements and security controls have been determined over time to provide the necessary protection for federal information and systems that are covered under FISMA. The tailoring criteria applied to the FIPS Publication 200 security requirements and the NIST Special Publication 800-53 security controls is ***not*** an endorsement for the elimination of those requirements and controls—rather, the tailoring criteria focuses on the protection of CUI from unauthorized disclosure in nonfederal systems and organizations. Moreover, since the security requirements are derivative from the NIST publications listed above, organizations should ***not*** assume that satisfying those particular requirements will automatically satisfy the security requirements and controls in FIPS Publication 200 and Special Publication 800-53.

In addition to the security objective of *confidentiality*, the objectives of *integrity* and *availability* remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program. While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives. Organizations that are interested in or required to comply with the recommendations in this publication are strongly advised to review the complete listing of security controls in the moderate baseline in Appendix E to ensure that their individual security plans and security control deployments provide the necessary and sufficient protection to address the cyber and kinetic threats to organizational missions and business operations. Addressing such threats is important because of the dependence these organizations have on their information technology infrastructures for their mission and business success.

EXPECTATIONS FOR THIS PUBLICATION

Executive Order 13556, *Controlled Unclassified Information*, November 4, 2010, establishes that the Controlled Unclassified Information (CUI) Executive Agent designated as the National Archives and Records Administration (NARA), shall develop and issue such directives as are necessary to implement the CUI Program. Consistent with this tasking and with the CUI Program's mission to establish uniform policies and practices across the federal government, NARA is issuing a final federal regulation in 2016 to establish the required controls and markings for CUI government-wide. This federal regulation, once enacted, will bind agencies throughout the executive branch to uniformly apply the standard safeguards, markings, dissemination, and decontrol requirements established by the CUI Program.

With regard to *federal information systems*, requirements in the federal regulation for protecting CUI at the moderate confidentiality impact level will be based on applicable policies established by OMB and applicable governmentwide standards and guidelines issued by NIST. The regulation will not create these policies, standards, and guidelines which are already established by OMB and NIST. The regulation will, however, require adherence to the policies and use of the standards and guidelines in a consistent manner throughout the executive branch, thereby reducing current complexity for federal agencies and their nonfederal partners, including contractors.

In addition to defining safeguarding requirements for CUI within the federal government, NARA has taken steps to alleviate the potential impact of such requirements on nonfederal organizations by jointly developing with NIST, Special Publication 800-171 — and defining security requirements for protecting CUI in nonfederal systems and organizations. This approach will help nonfederal entities, including contractors, to comply with the security requirements using the systems and practices they already have in place, rather than trying to use government-specific approaches. It will also provide a standardized and uniform set of requirements for all CUI security needs, tailored to nonfederal systems, allowing nonfederal organizations to comply with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI.

Finally, NARA, in its capacity as the CUI Executive Agent, also plans to sponsor in 2017, a single Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the federal CUI regulation and Special Publication 800-171 to contractors. This will further promote standardization to benefit a substantial number of nonfederal organizations that are attempting to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from federal agencies for the same information gives rise to confusion and inefficiencies. The CUI FAR clause will also address verification and compliance requirements for the security requirements in NIST Special Publication 800-171. Until the formal process of establishing such a FAR clause takes place, the requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements. If necessary, Special Publication 800-171 will be updated to remain consistent with the federal CUI regulation and the FAR clause.

DEFINITION AND USAGE OF THE TERM INFORMATION SYSTEM

Unless otherwise specified by legislation, regulation, or governmentwide policy, the use of the term ***information system*** in this publication is replaced by the term ***system***. This change reflects a more broad-based, holistic definition of information systems that includes, for example: general purpose information systems; industrial and process control systems; cyber-physical systems; and individual devices that are part of the *Internet of Things*. As computing platforms and technologies are increasingly deployed ubiquitously worldwide and systems and components are connected through wired and wireless networks, the susceptibility of Controlled Unclassified Information to loss or compromise grows—as does the potential for adverse consequences resulting from such occurrences.

FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Organizations that have implemented or plan to implement the *NIST Framework for Improving Critical Infrastructure Cybersecurity* can find in Appendix D of this publication, a direct mapping of the Controlled Unclassified Information (CUI) security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001. These controls are also mapped to the specific categories and subcategories associated with Cybersecurity Framework core functions: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

ADDITIONAL RESOURCES

Mapping NIST Special Publication 800-53 security controls to the Cybersecurity Framework: https://www.nist.gov/file/372651.

Mapping NIST Special Publication 800-171 requirements to the Cybersecurity Framework: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

Table of Contents

Errata

This table contains changes that have been incorporated into Special Publication 800-171. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature.

DATE	TYPE	CHANGE	PAGE
11-28-2017	Editorial	CAUTIONARY NOTE call out box, third paragraph: Change "publications" to "publication"	iv
11-28-2017	Editorial	EXPECTATIONS FOR THIS PUBLICATION call out box, third paragraph: Change "in compliance" to "comply"	v
11-28-2017	Editorial	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY call out box: Remove "See http://www.nist.gov/cyberframework." Add hyperlink	vii
11-28-2017	Editorial	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY call out box: Change "Once identified, those controls can be located in" to "These controls are also mapped to"	vii
11-28-2017	Substantive	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY call out box: Add "Additional Resources – Mapping NIST Special Publication 800-53 security controls to the Cybersecurity Framework: https://www.nist.gov/file/372651. Mapping NIST Special Publication 800-171 requirements to the Cybersecurity Framework: https://www.nist.gov/cyberframework/industry-resources"	vii
11-28-2017	Editorial	Chapter One, Section 1.1, second paragraph, first bullet: Change "moderate confidentiality impact" to "moderate confidentiality"	2
11-28-2017	Editorial	Chapter One, Section 1.1: Replace Footnote 10 with "NIST Special Publication 800-171A provides assessment procedures to help organizations determine compliance to the security requirements in Chapter Three"	2
11-28-2017	Editorial	Chapter One, Section 1.1, fourth paragraph: Change "particular specified" to "specified"	3
11-28-2017	Editorial	Chapter One, Section 1.1, fifth paragraph: Change "as long as" to "if"	3
11-28-2017	Editorial	Chapter One, Section 1.1, fifth paragraph: Remove "all of"	3
11-28-2017	Editorial	Chapter Three, first paragraph: Change "through the use of" to "using"	8
11-28-2017	Editorial	Chapter Three, third paragraph: Change "whether or not" to "whether"	8
11-28-2017	Substantive	Chapter Three, after fourth paragraph: Add call out box "THE MEANING OF ORGANIZATIONAL SYSTEMS"	9
11-28-2017	Substantive	Chapter Three, Section 3.1, Basic Security Requirement 3.1.1: Change "or" to "and"	9
11-28-2017	Substantive	Chapter Three, Section 3.3, Basic Security Requirement 3.3.1: Remove ", protect,"	10
11-28-2017	Substantive	Chapter Three, Section 3.4, Derived Security Requirement 3.4.3: Change "approve/disapprove" to "approve or disapprove"	11
11-28-2017	Substantive	Chapter Three, Section 3.4, Derived Security Requirement 3.4.7: Change "and" to "or"	11
11-28-2017	Substantive	Chapter Three, Section 3.5, Basic Security Requirement 3.5.1: Change "or" to "and"	11
11-28-2017	Substantive	Chapter Three, Section 3.6, Basic Security Requirement 3.6.1: Remove "adequate"	12

DATE	TYPE	CHANGE	PAGE
11-28-2017	Substantive	Chapter Three, Section 3.7, Basic Security Requirement 3.7.2: Remove "effective"	12
11-28-2017	Substantive	Chapter Three, Section 3.9, Basic Security Requirement 3.9.2: Remove "CUI and"	13
11-28-2017	Editorial	Chapter Three, Section 3.10, Derived Security Requirement 3.10.6: Remove "(e.g., telework sites)"	13
11-28-2017	Substantive	Chapter Three, Section 3.14, Basic Security Requirement 3.14.1: Remove "information and"	15
11-28-2017	Substantive	Chapter Three, Section 3.14, Basic Security Requirement 3.14.3: Remove "appropriate"	15
11-28-2017	Editorial	Chapter Three, Section 3.14, Basic Security Requirement 3.14.3: Change "actions" to "action"	15
11-28-2017	Editorial	Appendix A, References: Add URL to 32 CFR Part 2002, Controlled Unclassified Information	17
11-28-2017	Substantive	Appendix A, References: Add "National Institute of Standards and Technology Special Publication 800-171A (Draft), *Assessing Security Requirements for Controlled Unclassified Information*"	17
11-28-2017	Substantive	Appendix D, Table D-1, Basic Security Requirement 3.1.1: Change "or" to "and"	29
11-28-2017	Substantive	Appendix D, Table D-3, Basic Security Requirement 3.3.1: Remove ", protect,"	33
11-28-2017	Editorial	Appendix D, Table D-3, Basic Security Requirement 3.3.1: Add AU-11 to SP 800-53 mapping	33
11-28-2017	Substantive	Appendix D, Table D-4, Derived Security Requirement 3.4.3: Change "approve/disapprove" to "approve or disapprove"	35
11-28-2017	Substantive	Appendix D, Table D-4, Derived Security Requirement 3.4.7: Change "and" to "or"	36
11-28-2017	Editorial	Appendix D, Table D-4, Derived Security Requirement 3.4.7: Add "programs"	36
11-28-2017	Editorial	Appendix D, Table D-5, Basic Security Requirement 3.5.1: Add IA-3 to SP 800-53 mapping	37
11-28-2017	Substantive	Appendix D, Table D-5, Basic Security Requirement 3.5.1: Change "or" to "and"	37
11-28-2017	Substantive	Appendix D, Table D-6, Basic Security Requirement 3.6.1: Remove "adequate"	39
11-28-2017	Substantive	Appendix D, Table D-6, Derived Security Requirement 3.6.3: Remove IR-3(2) from SP 800-53 mapping	39
11-28-2017	Substantive	Appendix D, Table D-7, Basic Security Requirement 3.7.2: Remove "effective"	40
11-28-2017	Substantive	Appendix D, Table D-8, Derived Security Requirement 3.8.6: Change "information" to "CUI"	41
11-28-2017	Substantive	Appendix D, Table D-9, Basic Security Requirement 3.9.2: Remove "CUI and"	43
11-28-2017	Editorial	Appendix D, Table D-10, Basic Security Requirement 3.10.2: Add PE-4 to SP 800-53 mapping	44
11-28-2017	Editorial	Appendix D, Table D-10, Derived Security Requirement 3.10.6: Remove "(e.g., telework sites)"	44
11-28-2017	Substantive	Appendix D, Table D-14, Basic Security Requirement 3.14.1: Remove "information and"	50

DATE	TYPE	CHANGE	PAGE
11-28-2017	Substantive	Appendix D, Table D-14, Basic Security Requirement 3.14.3: Remove “appropriate”	50
11-28-2017	Editorial	Appendix D, Table D-14, Basic Security Requirement 3.14.3: Change “actions” to “action”	50
11-28-2017	Editorial	Appendix E, Table E-7, IA-3: Change “NCO” to “CUI”	58
11-28-2017	Editorial	Appendix E, Table E-8, IR-3(2): Change “CUI” to “NCO”	59
11-28-2017	Editorial	Appendix E, Table E-11, PE-4: Change “NFO” to “CUI”	62

CHAPTER ONE

INTRODUCTION

THE NEED TO PROTECT CONTROLLED UNCLASSIFIED INFORMATION

Today, more than at any time in history, the federal government is relying on external service providers to help carry out a wide range of federal missions and business functions using state-of-the-practice information systems.[1] Many federal contractors, for example, routinely process, store, and transmit sensitive federal information in their systems to support the delivery of essential products and services to federal agencies (e.g., providing credit card and other financial services; providing Web and electronic mail services; conducting background investigations for security clearances; processing healthcare data; providing cloud services; and developing communications, satellite, and weapons systems). Additionally, federal information is frequently provided to or shared with entities such as State and local governments, colleges and universities, and independent research organizations. The protection of sensitive federal information while residing in *nonfederal systems*[2] and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations, including those missions and functions related to the critical infrastructure.

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a disciplined and structured process for identifying the different types of information that are routinely used by federal agencies. On November 4, 2010, the President signed Executive Order 13556, *Controlled Unclassified Information*. The Executive Order established a governmentwide Controlled Unclassified Information (CUI)[3] Program to standardize the way the executive branch handles unclassified information that requires protection and designated the National Archives and Records Administration (NARA) as the Executive Agent[4] to implement that program. Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.

The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI *Registry*. The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent. Among other information, the CUI Registry identifies approved CUI categories and subcategories, provides

[1] An *information system* is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems for example, industrial/process control systems, cyber-physical systems, embedded systems, and devices. The term *system* is used throughout this publication to represent all types of computing platforms that can process, store, or transmit CUI.

[2] 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. A system that does not meet such criteria is a *nonfederal system*.

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

[4] NARA has delegated this authority to the Information Security Oversight Office, which is a component of NARA.

general descriptions for each, identifies the basis for controls, and sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

Executive Order 13556 also required that the CUI Program emphasize openness, transparency, and uniformity of governmentwide practices, and that the implementation of the program take place in a manner consistent with applicable policies established by the Office of Management and Budget (OMB) and federal standards and guidelines issued by the National Institute of Standards and Technology (NIST). The federal CUI *regulation*,[5] developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI, establishes self-inspection and oversight requirements, and delineates other facets of the program.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the *confidentiality* of CUI when the CUI is resident in a nonfederal system and organization; when the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[6] and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.[7] The security requirements apply *only* to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.[8] The security requirements are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR),[9] the CUI Executive Agent will address determining compliance with security requirements.[10]

In accordance with the federal CUI regulation, federal agencies using federal systems to process, store, or transmit CUI, as a minimum, must comply with:

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality);[11]

[5] 32 CFR Part 2002, *Controlled Unclassified Information*, issued September 14, 2016; effective November 14, 2016.

[6] 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, including the requirements in FIPS Publication 200 and the security controls in NIST Special Publication 800-53 (See 44 USC 3554(a)(1)(A)).

[7] The requirements in this publication can be used to comply with the FISMA requirement for senior agency officials to provide information security for the information that supports the operations and assets under their control, including CUI that is resident in nonfederal systems and organizations (See 44 USC 3554(a)(1)(A) and 3554(a)(2)).

[8] System *components* include, for example: mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.

[9] NARA, in its capacity as the CUI Executive Agent, plans to sponsor in 2017, a single FAR clause that will apply the requirements of the federal CUI regulation and NIST Special Publication 800-171 to contractors. Until the formal process of establishing such a single FAR clause takes place, the security requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

[10] NIST Special Publication 800-171A provides assessment procedures to help organizations determine compliance to the security requirements in Chapter Three.

[11] FIPS Publication 199 defines three values of potential impact (i.e., low, moderate, high) on organizations, assets, or individuals should there be a breach of security (e.g., a loss of confidentiality). The potential impact is *moderate* if the loss of confidentiality could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.

- Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; and
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories.*[12]

The responsibility of federal agencies to protect and ensure the control of CUI does not change when such information is shared with nonfederal partners. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by *nonfederal organizations* using nonfederal systems.[13] The specific requirements for safeguarding CUI in nonfederal systems and organizations are derived from the above authoritative federal standards and guidelines to maintain a consistent level of protection. However, recognizing that the scope of the safeguarding requirements in the federal CUI regulation is limited to the security objective of confidentiality (i.e., not directly addressing integrity and availability) and that some of the security requirements expressed in the NIST standards and guidelines are uniquely federal, the requirements in this publication have been *tailored* for nonfederal entities.

The tailoring criteria, described in Chapter Two, are not intended to reduce or minimize the federal requirements for the safeguarding of CUI as expressed in the federal CUI regulation. Rather, the intent is to express the requirements in a manner that allows for and facilitates the equivalent safeguarding measures within nonfederal systems and organizations and does not diminish the level of protection of CUI required for moderate confidentiality. Additional or differing requirements other than those requirements described in this publication may be applied only when such requirements are based on law, regulation, or governmentwide policy and when indicated in the CUI Registry as CUI-specified. The provision of safeguarding requirements for CUI in a specified category will be addressed by NARA in its CUI guidance and in the CUI FAR, and reflected as specific requirements in contracts or other agreements.

If nonfederal organizations entrusted with protecting CUI designate systems or components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements to only those systems or components. Isolating CUI into its own *security domain* by applying architectural design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices) may be the most cost-effective and efficient approach for nonfederal organizations to satisfy the security requirements and protect the confidentiality of CUI. Security domains may employ physical separation, logical separation, or a combination of both. This approach can reasonably provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond which it typically requires for protecting its missions, operations, and assets. Nonfederal organizations may choose to use the same CUI infrastructure for multiple government contracts or agreements, if the CUI infrastructure meets the safeguarding requirements for the organization's CUI-related contracts and/or agreements including any specific safeguarding required or permitted by the authorizing law, regulation, or governmentwide policy.

[12] NIST Special Publication 800-60 is under revision to align with the CUI categories and subcategories in the CUI Registry.

[13] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system. Examples include: State, local, and tribal governments; colleges and universities; and contractors.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of individuals and organizations in both the public and private sectors including, but not limited to:

- 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); and
- Individuals with security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

The above roles and responsibilities can be viewed from two distinct perspectives: the *federal perspective* as the entity establishing and conveying the security requirements in contractual vehicles or other types of inter-organizational agreements; and the *nonfederal perspective* as the entity responding to and complying with the security requirements set forth in contracts or agreements.

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI; the format and structure of the requirements; and the tailoring criteria applied to the NIST standards and guidelines to obtain the requirements.
- **Chapter Three** describes the fourteen families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.
- **Supporting appendices** provide additional information related to the protection of CUI in nonfederal systems and organizations including: general references; definitions and terms; acronyms; mapping tables relating security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001; and an explanation of the tailoring actions employed on the moderate security control baseline.

CHAPTER TWO

THE FUNDAMENTALS

ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING SECURITY REQUIREMENTS

This chapter describes the assumptions and methodology used to develop the security requirements to protect CUI in nonfederal systems and organizations; the structure of the basic and derived security requirements; and the tailoring criteria applied to the federal information security requirements and controls.

2.1 BASIC ASSUMPTIONS

The security requirements described in this publication have been developed based on three fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations; and
- The confidentiality impact value for CUI is no less than *moderate*[14] in accordance with Federal Information Processing Standards (FIPS) Publication 199.[15]

The above assumptions reinforce the concept that federal information designated as CUI has the same intrinsic *value* and potential *adverse impact* if compromised—whether such information resides in a federal or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies and the economic and national security interests of the nation. Additional assumptions also impacting the development of the security requirements and the expectation of federal agencies in working with nonfederal entities include:

- Nonfederal organizations have information technology infrastructures in place, and are not necessarily developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI;
- Nonfederal organizations have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the security requirements;
- Nonfederal organizations can implement a variety of potential security solutions either directly or through the use of managed services, to satisfy security requirements; and
- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.

[14] The moderate impact *value* defined in FIPS Publication 199 may become part of a moderate impact *system* in FIPS Publication 200, which in turn, requires the use of the moderate security control baseline in NIST Special Publication 800-53 as the starting point for tailoring actions.

[15] In accordance with 32 CFR 2002(g), CUI is categorized at no less than the moderate confidentiality impact value. However, when federal law, regulation, or govenmentwide policy establishing the control of the CUI specifies controls that differ from those of the moderate confidentiality baseline, then these will be followed.

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the security requirements contained in this publication are consistent with and complementary to the standards and guidelines used by federal agencies to protect CUI.

2.2 DEVELOPMENT OF SECURITY REQUIREMENTS

The security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations have a well-defined structure that consists of a *basic security requirements* section and a *derived security requirements* section. The basic security requirements are obtained from FIPS Publication 200, which provides the high-level and fundamental security requirements for federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53. Starting with the FIPS Publication 200 security requirements and the security controls in the moderate baseline (i.e., the minimum level of protection required for CUI in federal systems and organizations), the requirements and controls are *tailored* to eliminate requirements, controls, or parts of controls that are:

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.[16]

Appendix E provides a complete listing of security controls that support the CUI derived security requirements and those controls that have been eliminated from the NIST Special Publication 800-53 moderate baseline based on the CUI tailoring criteria described above.

The combination of the basic and derived security requirements captures the intent of FIPS Publication 200 and NIST Special Publication 800-53, with respect to the protection of the *confidentiality* of CUI in nonfederal systems and organizations. Appendix D provides informal mappings of the security requirements to the relevant security controls in NIST Special Publication 800-53 and ISO/IEC 27001. The mappings promote a better understanding of the security requirements and are *not* intended to impose additional requirements on nonfederal organizations.

The following example taken from the *Configuration Management* family illustrates the structure of a typical security requirement:

[16] The security requirements developed from the tailored FIPS Publication 200 security requirements and the NIST Special Publication 800-53 moderate security control baseline represent a subset of the safeguarding measures that are necessary for a *comprehensive* information security program. The strength and quality of such programs in nonfederal organizations depend on the degree to which the organizations implement the security requirements and controls that are expected to be routinely satisfied without specification by the federal government. This includes implementing security policies, procedures, and practices that support an effective risk-based information security program. Nonfederal organizations are encouraged to refer to Appendix E and Special Publication 800-53 for a complete listing of security controls in the moderate baseline deemed out of scope for the security requirements in Chapter Three.

Basic Security Requirements

- Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- Establish and enforce security configuration settings for information technology products employed in organizational systems.

Derived Security Requirements

- Track, review, approve or disapprove, and audit changes to systems.
- Analyze the security impact of changes prior to implementation.
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to systems.
- Employ the principle of least functionality by configuring systems to provide only essential capabilities.
- Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Control and monitor user-installed software.

For ease of use, the security requirements are organized into fourteen *families*. Each family contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum-security requirements for federal information and systems described in FIPS Publication 200. The *contingency planning*, *system and services acquisition*, and *planning* requirements are not included within the scope of this publication due to the aforementioned tailoring criteria.[17] Table 1 lists the security requirement families addressed in this publication.

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

[17] Three exceptions include: a requirement to protect the confidentiality of system backups (derived from CP-9) from the *contingency planning* family; a requirement to develop and implement a system security plan (derived from PL-2) from the *planning* family; and a requirement to implement system security engineering principles (derived from SA-8) from the *system and services acquisition* family. For convenience, these requirements are included with the CUI *media protection*, *security assessment*, and *system and communications protection* requirements families, respectively.

CHAPTER THREE

THE REQUIREMENTS

SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

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

Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

When requested, the system security plan and any associated plans of action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

The security requirements in this publication should be applied to the nonfederal organization's internal systems processing, storing, or transmitting CUI. Some systems, including specialized systems (e.g., industrial/process control systems, Computer Numerical Control machines, medical devices), may have restrictions or limitations on the application of certain security requirements.

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

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

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

To accommodate such issues, the system security plan, as reflected in Requirement 3.12.4, should be used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies should be managed though plans of action, as reflected in Requirement 3.12.2.

THE MEANING OF ORGANIZATIONAL SYSTEMS

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

3.1 ACCESS CONTROL

Basic Security Requirements

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

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

Derived Security Requirements

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

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

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

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

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

3.1.8 Limit unsuccessful logon attempts.

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

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

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

3.1.12 Monitor and control remote access sessions.

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

3.1.14 Route remote access via managed access control points.

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

3.1.16 Authorize wireless access prior to allowing such connections.

3.1.17 Protect wireless access using authentication and encryption.

3.1.18 Control connection of mobile devices.

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

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

3.1.21 Limit use of organizational portable storage devices on external systems.

3.1.22 Control CUI posted or processed on publicly accessible systems.

3.2 AWARENESS AND TRAINING

Basic Security Requirements

3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

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

Derived Security Requirements

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

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements

3.3.1 Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.

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

Derived Security Requirements

3.3.3 Review and update audited events.

3.3.4 Alert in the event of an audit process failure.

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

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

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

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

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

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

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

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

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

Derived Security Requirements

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

3.4.4 Analyze the security impact of changes prior to implementation.

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

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

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

3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.9 Control and monitor user-installed software.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements

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

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

Derived Security Requirements

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

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

3.5.5 Prevent reuse of identifiers for a defined period.

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

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

3.5.6 Disable identifiers after a defined period of inactivity.

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

3.5.8 Prohibit password reuse for a specified number of generations.

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

3.5.10 Store and transmit only cryptographically-protected passwords.

3.5.11 Obscure feedback of authentication information.

3.6 INCIDENT RESPONSE

Basic Security Requirements

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

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

Derived Security Requirements

3.6.3 Test the organizational incident response capability.

3.7 MAINTENANCE

Basic Security Requirements

3.7.1 Perform maintenance on organizational systems.[24]

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

Derived Security Requirements

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

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

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

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

3.8 MEDIA PROTECTION

Basic Security Requirements

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

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

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

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

Derived Security Requirements

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

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

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

3.8.7 Control the use of removable media on system components.

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

3.8.9 Protect the confidentiality of backup CUI at storage locations.

3.9 PERSONNEL SECURITY

Basic Security Requirements

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

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

Derived Security Requirements

None.

3.10 PHYSICAL PROTECTION

Basic Security Requirements

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

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

Derived Security Requirements

3.10.3 Escort visitors and monitor visitor activity.

3.10.4 Maintain audit logs of physical access.

3.10.5 Control and manage physical access devices.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

3.11 RISK ASSESSMENT

Basic Security Requirements

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

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

Derived Security Requirements

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

3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

3.12 SECURITY ASSESSMENT

Basic Security Requirements

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

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

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

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

Derived Security Requirements

None.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements

3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

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

Derived Security Requirements

3.13.3 Separate user functionality from system management functionality.

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

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

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

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

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

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

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

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

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

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

3.13.13 Control and monitor the use of mobile code.

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

3.13.15 Protect the authenticity of communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements

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

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

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

Derived Security Requirements

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

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

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

3.14.7 Identify unauthorized use of organizational systems.

[27] Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

NARA, SECURITY REQUIREMENTS, AND THE FAR CLAUSE

Executive Order 13556, *Controlled Unclassified Information*, November 4, 2010, established the CUI Program and designated the National Archives and Record Administration (NARA) as its Executive Agent to implement the Order and to oversee agency actions to ensure compliance with the Order. The CUI Executive Agent anticipates establishing a single Federal Acquisition Regulation (FAR) clause in 2017 to apply the security requirements of NIST Special Publication 800-171 to contractor environments as well as to determine oversight responsibilities and requirements. The Executive Agent also addresses its oversight of federal agencies in the 32 CFR Part 2002. The approaches to federal oversight will be determined through the uniform CUI FAR clause, future understandings, and any agreements between federal agencies and their nonfederal information-sharing partners.

APPENDIX A

REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES[28]

LEGISLATION, EXECUTIVE ORDERS, AND REGULATIONS

1. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014. http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
2. Executive Order 13556, *Controlled Unclassified Information*, November 2010. http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
3. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
4. 32 CFR Part 2002, *Controlled Unclassified Information*, September 2016. https://www.gpo.gov/fdsys/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

STANDARDS, GUIDELINES, AND INSTRUCTIONS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199 (as amended), *Standards for Security Categorization of Federal Information and Information Systems*. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200 (as amended), *Minimum Security Requirements for Federal Information and Information Systems*. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
3. National Institute of Standards and Technology Special Publication 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r4
4. National Institute of Standards and Technology Special Publication 800-60 (as amended), *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 1. https://doi.org/10.6028/NIST.SP.800-60v1r1
5. National Institute of Standards and Technology Special Publication 800-60 (as amended), *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 2. https://csrc.nist.gov/publications/detail/sp/800-193/draft https://doi.org/10.6028/NIST.SP.800-60v2r1
6. National Institute of Standards and Technology Special Publication 800-171A (Draft), *Assessing Security Requirements for Controlled Unclassified Information*. https://csrc.nist.gov/publications/detail/sp/800-171a/draft

[28] References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

7. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (as amended). https://www.nist.gov/cyberframework

8. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, September 2013.

9. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, September 2013.

10. Committee on National Security Systems Instruction 4009 (as amended), *National Information Assurance Glossary*. https://www.cnss.gov

OTHER RESOURCES

1. National Archives and Records Administration, *Controlled Unclassified Information Registry*. https://www.archives.gov/cui/registry/category-list

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-171. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

agency	See *executive agency*.
assessment	See *Security Control Assessment*.
assessor	See *Security Control Assessor*.
audit log	A chronological record of system activities, including records of system accesses and operations performed in a given period.
audit record	An individual entry in an audit log related to an audited event.
authentication [FIPS 200, Adapted]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
baseline configuration	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
blacklisting	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
configuration settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
controlled area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

controlled unclassified information [E.O. 13556]	Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
CUI categories or subcategories [Title 32 CFR, Part 2002]	Those types of information for which laws, regulations, or governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.
CUI Executive Agent [Title 32 CFR, Part 2002]	The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
CUI program [Title 32 CFR, Part 2002]	The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.
CUI registry [Title 32 CFR, Part 2002]	The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
environment of operation [NIST SP 800-37, Adapted]	The physical surroundings in which a system processes, stores, and transmits information.
executive agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 105; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
external system (or component)	A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
external system service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

external system service provider	A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
external network	A network not controlled by the organization.
federal agency	See *executive agency*.
federal information system [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
FIPS-validated cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-Approved Cryptography*.
firmware	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
hardware	The physical components of a system. See *Software* and *Firmware*.
identifier	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.
impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.
impact value	The assessed potential impact resulting from a compromise of the confidentiality of information (e.g., CUI) expressed as a value of low, moderate, or high.
incident [FIPS 200, Adapted]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

information flow control	Procedure to ensure that information transfers within a system are not made in violation of the security policy.
information resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
information security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information system [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
information technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
insider threat	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.
integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
internal network	A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
least privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

local access	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.
mobile code	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.
mobile device	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.
multifactor authentication	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See also *Authenticator*.
nonfederal organization	An entity that owns, operates, or maintains a nonfederal system.
nonfederal system	A system that does not meet the criteria for a federal system.
network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
network access	Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
nonlocal maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.

on behalf of (an agency) [32 CFR Part 2002]	A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure.
portable storage device	A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).
potential impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
privileged account	A system account with authorizations of a privileged user.
privileged user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
remote access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
remote maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
replay resistance	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation.
risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
security assessment	See *Security Control Assessment*.
security control [FIPS 199, Adapted]	A safeguard or countermeasure prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
security control assessment [CNSSI 4009, Adapted]	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for a system or organization.
security functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational systems or the environments in which those systems operate.
security functions	The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

security relevance	Functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.
split tunneling	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.
supplemental guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
system	See *Information System*.
system component [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.
system security plan	A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. In particular, the system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
system service	A capability provided by a system that facilitates information processing, storage, or transmission.
threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
user [CNSSI 4009, Adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
whitelisting	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.
wireless technology	Technology that permits the transfer of information between separated points without physical connection.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
ITL	Information Technology Laboratory
NARA	National Archives and Records Administration
NFO	Nonfederal Organization
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication

APPENDIX D

MAPPING TABLES

MAPPING SECURITY REQUIREMENTS TO SECURITY CONTROLS

Tables D-1 through D-14 provide a mapping of the security requirements to the relevant security controls in NIST Special Publication 800-53. The mapping tables are included for informational purposes only and are not intended to convey or impart any additional security requirements beyond those requirements defined in Chapter Three. Moreover, because the security controls were developed for federal agencies, the supplemental guidance associated with those controls may not be applicable to nonfederal organizations. In some cases, the relevant security controls include additional expectations beyond those required to protect CUI and have been tailored using the criteria in Chapter Two. Only the portion of the security control relevant to the security requirement is applicable. The tables also include a secondary mapping of the security controls from Special Publication 800-53 to the relevant controls in ISO/IEC 27001, Annex A. The NIST to ISO/IEC mapping is obtained from Special Publication 800-53, Appendix H. An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control. It is also important to note that, due to the tailoring for CUI, satisfaction of a basic or derived security requirement does *not* mean that the corresponding security control or control enhancement from NIST Special Publication 800-53 has been met, since certain elements of the control or control enhancement that are not essential to protecting the confidentiality of CUI are not reflected in those requirements.

Organizations that have implemented or plan to implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity* can use the mapping of the security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001 to locate the equivalent controls in the categories and subcategories associated with the core functions of the Framework: identify, protect, detect, respond, and recover. The security control mapping information can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). **3.1.2** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
Derived Security Requirements				
3.1.3 Control the flow of CUI in accordance with approved authorizations.	AC-4	Information Flow Enforcement	A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	A.6.1.2	Segregation of duties
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	A.9.1.2	Access to networks and network services
			A.9.2.3	Management of privileged access rights
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
	AC-6(1)	Least Privilege *Authorize Access to Security Functions*	*No direct mapping.*	
	AC-6(5)	Least Privilege *Privileged Accounts*	*No direct mapping.*	
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege *Non-Privileged Access for Nonsecurity Functions*	*No direct mapping.*	
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC-6(9)	Least Privilege *Auditing Use of Privileged Functions*	*No direct mapping.*	
	AC-6(10)	Least Privilege *Prohibit Non-Privileged Users from Executing Privileged Functions*	*No direct mapping.*	
3.1.8 Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	A.9.4.2	Secure logon procedures
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	AC-8	System Use Notification	A.9.4.2	Secure logon procedures
3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	AC-11	Session Lock	A.11.2.8	Unattended user equipment
			A.11.2.9	Clear desk and clear screen policy
	AC-11(1)	Session Lock *Pattern-Hiding Displays*	*No direct mapping.*	
3.1.11 Terminate (automatically) a user session after a defined condition.	AC-12	Session Termination	*No direct mapping.*	
3.1.12 Monitor and control remote access sessions.	AC-17(1)	Remote Access *Automated Monitoring / Control*	*No direct mapping.*	

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	Remote Access *Protection of Confidentiality / Integrity Using Encryption*	*No direct mapping.*	
3.1.14 Route remote access via managed access control points.	AC-17(3)	Remote Access *Managed Access Control Points*	*No direct mapping.*	
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4)	Remote Access *Privileged Commands / Access*	*No direct mapping.*	
3.1.16 Authorize wireless access prior to allowing such connections.	AC-18	Wireless Access	A.6.2.1	Mobile device policy
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
3.1.17 Protect wireless access using authentication and encryption.	AC-18(1)	Wireless Access *Authentication and Encryption*	*No direct mapping.*	
3.1.18 Control connection of mobile devices.	AC-19	Access Control for Mobile Devices	A.6.2.1	Mobile device policy
			A.11.2.6	Security of equipment and assets off-premises
			A.13.2.1	Information transfer policies and procedures
3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.	AC-19(5)	Access Control for Mobile Devices *Full Device / Container-Based Encryption*	*No direct mapping.*	
3.1.20 Verify and control/limit connections to and use of external systems.	AC-20	Use of External Systems	A.11.2.6	Security of equipment and assets off-premises
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
	AC-20(1)	Use of External Systems *Limits on Authorized Use*	*No direct mapping.*	
3.1.21 Limit use of organizational portable storage devices on external systems.	AC-20(2)	Use of External Systems *Portable Storage Devices*	*No direct mapping.*	
3.1.22 Control CUI posted or processed on publicly accessible systems.	AC-22	Publicly Accessible Content	*No direct mapping.*	

TABLE D-2: MAPPING AWARENESS AND TRAINING REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.2 AWARENESS AND TRAINING				
Basic Security Requirements				
3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
			A.12.2.1	Controls against malware
3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
Derived Security Requirements				
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	*No direct mapping.*	

TABLE D-3: MAPPING AUDIT AND ACCOUNTABILITY REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.3 AUDIT AND ACCOUNTABILITY				
Basic Security Requirements				
3.3.1 Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	AU-2	Audit Events	*No direct mapping.*	
	AU-3	Content of Audit Records	A.12.4.1*	Event logging
	AU-3(1)	Content of Audit Records *Additional Audit Information*	*No direct mapping.*	
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	AU-6	Audit Review, Analysis, and Reporting	A.12.4.1	Event logging
			A.16.1.2	Reporting information security events
			A.16.1.4	Assessment of and decision on information security events
	AU-11	Audit Record Retention	A.12.4.1	Event logging
			A.12.4.3	Administrator and operator logs
	AU-12	Audit Generation	A.12.4.1	Event logging
			A.16.1.7	Collection of evidence
Derived Security Requirements				
3.3.3 Review and update audited events.	AU-2(3)	Audit Events *Reviews and Updates*	*No direct mapping.*	
3.3.4 Alert in the event of an audit process failure.	AU-5	Response to Audit Processing Failures	*No direct mapping.*	
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(3)	Audit Review, Analysis, and Reporting *Correlate Audit Repositories*	*No direct mapping.*	
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.	AU-7	Audit Reduction and Report Generation	*No direct mapping.*	
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU-8	Time Stamps	A.12.4.4	Clock synchronization
	AU-8(1)	Time Stamps *Synchronization with Authoritative Time Source*	*No direct mapping.*	
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9	Protection of Audit Information	A.12.4.2	Protection of log information
			A.12.4.3	Administrator and operator logs
			A.18.1.3	Protection of records

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*
3.3.9 Limit management of audit functionality to a subset of privileged users.	AU-9(4)	Protection of Audit Information *Access by Subset of Privileged Users*	*No direct mapping.*

TABLE D-4: MAPPING CONFIGURATION MANAGEMENT REQUIREMENTS TO CONTROLS[29]

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.4 CONFIGURATION MANAGEMENT				
Basic Security Requirements				
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. **3.4.2** Establish and enforce security configuration settings for information technology products employed in organizational systems.	CM-2	Baseline Configuration	*No direct mapping.*	
	CM-6	Configuration Settings	*No direct mapping.*	
	CM-8	System Component Inventory	A.8.1.1	Inventory of assets
			A.8.1.2	Ownership of assets
	CM-8(1)	System Component Inventory *Updates During Installations / Removals*	*No direct mapping.*	
Derived Security Requirements				
3.4.3 Track, review, approve or disapprove, and audit changes to organizational systems.	CM-3	Configuration Change Control	A.12.1.2	Change management
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.14.2.4	Restrictions on changes to software packages
3.4.4 Analyze the security impact of changes prior to implementation.	CM-4	Security Impact Analysis	A.14.2.3	Technical review of applications after operating platform changes
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CM-5	Access Restrictions for Change	A.9.2.3	Management of privileged access rights
			A.9.4.5	Access control to program source code
			A.12.1.2	Change management
			A.12.1.4	Separation of development, testing, and operational environments
			A.12.5.1	Installation of software on operational systems

[29] CM-7(5), the least functionality whitelisting policy, is listed as an alternative to CM-7(4), the least functionality blacklisting policy, for organizations desiring greater protection for systems containing CUI. CM-7(5) is only required in federal systems at the high security control baseline in accordance with NIST Special Publication 800-53.

SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	CM-7	Least Functionality	A.12.5.1*	Installation of software on operational systems
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	CM-7(1)	Least Functionality *Periodic Review*	*No direct mapping.*	
		CM-7(2)	Least Functionality *Prevent program execution*	*No direct mapping.*	
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	CM-7(4)	Least Functionality *Unauthorized Software/ Blacklisting*	*No direct mapping.*	
		CM-7(5)	Least Functionality *Authorized Software/ Whitelisting*	*No direct mapping.*	
3.4.9	Control and monitor user-installed software.	CM-11	User-Installed Software	A.12.5.1	Installation of software on operational systems
				A.12.6.2	Restrictions on software installation

TABLE D-5: MAPPING IDENTIFICATION AND AUTHENTICATION REQUIREMENTS TO CONTROLS[30]

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5 IDENTIFICATION AND AUTHENTICATION				
Basic Security Requirements				
3.5.1 Identify system users, processes acting on behalf of users, and devices.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	IA-3	Device Identification and Authentication	*No direct mapping.*	
	IA-5	Authenticator Management	A.9.2.1	User registration and de-registration
			A.9.2.4	Management of secret authentication information of users
			A.9.3.1	Use of secret authentication information
			A.9.4.3	Password management system
Derived Security Requirements				
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts*	*No direct mapping.*	
	IA-2(2)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts*	*No direct mapping.*	
	IA-2(3)	Identification and Authentication (Organizational Users) *Local Access to Privileged Accounts*	*No direct mapping.*	
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts-Replay Resistant*	*No direct mapping.*	
	IA-2(9)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts-Replay Resistant*	*No direct mapping.*	

[30] IA-2(9) is *not* currently in the NIST Special Publication 800-53 moderate security control baseline although it will be added to the baseline in the next update. Employing multifactor authentication without a replay-resistant capability for non-privileged accounts creates a significant vulnerability for systems transmitting CUI.

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5.5 Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
3.5.6 Disable identifiers after a defined period of inactivity.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	Authenticator Management *Password-Based Authentication*	*No direct mapping.*	
3.5.8 Prohibit password reuse for a specified number of generations.				
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.				
3.5.10 Store and transmit only cryptographically-protected passwords.				
3.5.11 Obscure feedback of authentication information.	IA-6	Authenticator Feedback	A.9.4.2	Secure logon procedures

TABLE D-6: MAPPING INCIDENT RESPONSE REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.6 INCIDENT RESPONSE				
Basic Security Requirements				
3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	IR-2	Incident Response Training	A.7.2.2*	Information security awareness, education, and training
	IR-4	Incident Handling	A.16.1.4	Assessment of and decision on information security events
			A.16.1.5	Response to information security incidents
			A.16.1.6	Learning from information security incidents
	IR-5	Incident Monitoring	*No direct mapping.*	
3.6.2 Track, document, and report incidents to appropriate organizational officials and/or authorities.	IR-6	Incident Reporting	A.6.1.3	Contact with authorities
			A.16.1.2	Reporting information security events
	IR-7	Incident Response Assistance	*No direct mapping.*	
Derived Security Requirements				
3.6.3 Test the organizational incident response capability.	IR-3	Incident Response Testing	*No direct mapping.*	

TABLE D-7: MAPPING MAINTENANCE REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.7 MAINTENANCE				
Basic Security Requirements				
3.7.1 Perform maintenance on organizational systems.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA-3	Maintenance Tools	*No direct mapping.*	
	MA-3(1)	Maintenance Tools *Inspect Tools*	*No direct mapping.*	
	MA-3(2)	Maintenance Tools *Inspect media*	*No direct mapping.*	
Derived Security Requirements				
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	MA-3(2)	Maintenance Tools	*No direct mapping.*	
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA-4	Nonlocal Maintenance	*No direct mapping.*	
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Maintenance Personnel	*No direct mapping.*	

TABLE D-8: MAPPING MEDIA PROTECTION REQUIREMENTS TO CONTROLS[31]

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8 MEDIA PROTECTION				
Basic Security Requirements				
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP-2	Media Access	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
3.8.2 Limit access to CUI on system media to authorized users.	MP-4	Media Storage	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.			A.11.2.9	Clear desk and clear screen policy
	MP-6	Media Sanitization	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.2	Disposal of media
			A.11.2.7	Secure disposal or reuse of equipment
Derived Security Requirements				
3.8.4 Mark media with necessary CUI markings and distribution limitations.	MP-3	Media Marking	A.8.2.2	Labelling of Information
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	Media Transport	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.3	Physical media transfer
			A.11.2.5	Removal of assets
			A.11.2.6	Security of equipment and assets off-premises
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport *Cryptographic Protection*	*No direct mapping.*	
3.8.7 Control the use of removable media on system components.	MP-7	Media Use	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media

[31] CP-9, *Information System Backup*, is included with the Media Protection family since the Contingency Planning family was not included in the security requirements.

SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	Media Use *Prohibit Use Without Owner*	*No direct mapping.*	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	CP-9	System Backup	A.12.3.1	Information backup
				A.17.1.2	Implementing information security continuity
				A.18.1.3	Protection of records

TABLE D-9: MAPPING PERSONNEL SECURITY REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.9 PERSONNEL SECURITY				
Basic Security Requirements				
3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	PS-3	Personnel Screening	A.7.1.1	Screening
	PS-4	Personnel Termination	A.7.3.1	Termination or change of employment responsibilities
3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.			A.8.1.4	Return of assets
	PS-5	Personnel Transfer	A.7.3.1	Termination or change of employment responsibilities
			A.8.1.4	Return of assets
Derived Security Requirements	None.			

TABLE D-10: MAPPING PHYSICAL PROTECTION REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.10 PHYSICAL PROTECTION				
Basic Security Requirements				
3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. **3.10.2** Protect and monitor the physical facility and support infrastructure for organizational systems.	PE-2	Physical Access Authorizations	A.11.1.2*	Physical entry controls
	PE-4	Access Control for Transmission Medium	A.11.1.2	Physical entry controls
			A.11.2.3	Cabling security
	PE-5	Access Control for Output Devices	A.11.1.2	Physical entry controls
			A.11.1.3	Securing offices, rooms, and facilities
	PE-6	Monitoring Physical Access	*No direct mapping.*	
Derived Security Requirements				
3.10.3 Escort visitors and monitor visitor activity.	PE-3	Physical Access Control	A.11.1.1	Physical security perimeter
			A.11.1.2	Physical entry controls
3.10.4 Maintain audit logs of physical access.			A.11.1.3	Securing offices, rooms, and facilities
3.10.5 Control and manage physical access devices.				
3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	PE-17	Alternate Work Site	A.6.2.2	Teleworking
			A.11.2.6	Security of equipment and assets off-premises
			A.13.2.1	Information transfer policies and procedures

TABLE D-11: MAPPING RISK ASSESSMENT REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.11 RISK ASSESSMENT				
Basic Security Requirements				
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	RA-3	Risk Assessment	A.12.6.1*	Management of technical vulnerabilities
Derived Security Requirements				
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities
	RA-5(5)	Vulnerability Scanning *Privileged Access*	*No direct mapping.*	
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities

TABLE D-12: MAPPING SECURITY ASSESSMENT REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.12 SECURITY ASSESSMENT				
Basic Security Requirements				
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	CA-2	Security Assessments	A.14.2.8	System security testing
			A.18.2.2	Compliance with security policies and standards
			A.18.2.3	Technical compliance review
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	CA-5	Plan of Action and Milestones	*No direct mapping.*	
	CA-7	Continuous Monitoring	*No direct mapping.*	
3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	PL-2	System Security Plan	A.6.1.2	Information security coordination
3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.				
Derived Security Requirements	None.			

TABLE D-13: MAPPING SYSTEM AND COMMUNICATIONS PROTECTION REQUIREMENTS TO CONTROLS[32]

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13 SYSTEM AND COMMUNICATIONS PROTECTION				
Basic Security Requirements				
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	SA-8	Security Engineering Principles	A.14.2.5	Secure system engineering principles
Derived Security Requirements				
3.13.3 Separate user functionality from system management functionality.	SC-2	Application Partitioning	*No direct mapping.*	
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	Information in Shared Resources	*No direct mapping.*	
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC-7(5)	Boundary Protection *Deny by Default / Allow by Exception*	*No direct mapping.*	

[32] SA-8, *Security Engineering Principles*, is included with the System and Communications Protection family since the System and Services Acquisition family was not included in the security requirements.

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	SC-7(7)	Boundary Protection *Prevent Split Tunneling for Remote Devices*	*No direct mapping.*	
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8	Transmission Confidentiality and Integrity	A.8.2.3	Handling of Assets
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.13.2.3	Electronic messaging
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
	SC-8(1)	Transmission Confidentiality and Integrity *Cryptographic or Alternate Physical Protection*	*No direct mapping.*	
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SC-10	Network Disconnect	A.13.1.1	Network controls
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.	SC-12	Cryptographic Key Establishment and Management	A.10.1.2	Key Management
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	Cryptographic Protection	A.10.1.1	Policy on the use of cryptographic controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.5	Regulation of cryptographic controls
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	SC-15	Collaborative Computing Devices	A.13.2.1*	Information transfer policies and procedures
3.13.13 Control and monitor the use of mobile code.	SC-18	Mobile Code	*No direct mapping.*	

SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19	Voice over Internet Protocol	*No direct mapping.*	
3.13.15	Protect the authenticity of communications sessions.	SC-23	Session Authenticity	*No direct mapping.*	
3.13.16	Protect the confidentiality of CUI at rest.	SC-28	Protection of Information at Rest	A.8.2.3*	Handling of Assets

TABLE D-14: MAPPING SYSTEM AND INFORMATION INTEGRITY REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.14 SYSTEM AND INFORMATION INTEGRITY				
Basic Security Requirements				
3.14.1 Identify, report, and correct system flaws in a timely manner. **3.14.2** Provide protection from malicious code at appropriate locations within organizational systems. **3.14.3** Monitor system security alerts and advisories and take action in response.	SI-2	Flaw Remediation	A.12.6.1	Management of technical vulnerabilities
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.16.1.3	Reporting information security weaknesses
	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
	SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	Contact with special interest groups
Derived Security Requirements				
3.14.4 Update malicious code protection mechanisms when new releases are available.	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.				
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4	System Monitoring	*No direct mapping.*	
	SI-4(4)	System Monitoring *Inbound and Outbound Communications Traffic*	*No direct mapping.*	
3.14.7 Identify unauthorized use of organizational systems.	SI-4	System Monitoring	*No direct mapping.*	

APPENDIX E

TAILORING CRITERIA

LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a complete listing of the security controls in the NIST Special Publication 800-53 moderate baseline, one of the sources along with FIPS Publication 200, for the security requirements described in Chapter Three. Tables E-1 through E-17 contain the tailoring actions (by family) that have been carried out on the security controls in the moderate baseline in accordance with the tailoring criteria established by NIST and NARA.[33] The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements obtained from the security requirements in FIPS Publication 200.[34]

There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;[35] or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.[36]

The following symbols are used in Tables E-1 through E-17 to specify the particular tailoring actions taken or when no tailoring actions were required.

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

[33] Organizations can use the information in Appendix E to build a CUI confidentiality *overlay* as defined in NIST Special Publication 800-53, Appendix I.

[34] The same *tailoring criteria* were applied to the security requirements in FIPS Publication 200 resulting in the CUI basic security requirements in described in Chapter Three and Appendix D.

[35] While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between the security objectives of confidentiality and integrity. Therefore, most of security controls in the NIST Special Publication 800-53 moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.

[36] The security controls tailored out of the moderate baseline in Special Publication 800-53 with regard to the protection of CUI (i.e., controls specifically marked as either NCO or NFO in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

TABLE E-1: TAILORING ACTIONS FOR ACCESS CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
AC-1	Access Control Policy and Procedures	NFO
AC-2	Account Management	CUI
AC-2(1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	NCO
AC-2(2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	NCO
AC-2(3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*	NCO
AC-2(4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*	NCO
AC-3	Access Enforcement	CUI
AC-4	Information Flow Enforcement	CUI
AC-5	Separation of Duties	CUI
AC-6	Least Privilege	CUI
AC-6(1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	CUI
AC-6(2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*	CUI
AC-6(5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*	CUI
AC-6(9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*	CUI
AC-6(10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*	CUI
AC-7	Unsuccessful Logon Attempts	CUI
AC-8	System Use Notification	CUI
AC-11	Session Lock	CUI
AC-11(1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*	CUI
AC-12	Session Termination	CUI
AC-14	Permitted Actions without Identification or Authentication	FED
AC-17	Remote Access	CUI
AC-17(1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*	CUI
AC-17(2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*	CUI
AC-17(3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*	CUI
AC-17(4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*	CUI
AC-18	Wireless Access	CUI
AC-18(1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*	CUI
AC-19	Access Control for Mobile Devices	CUI
AC-19(5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*	CUI
AC-20	Use of External Systems	CUI
AC-20(1)	*USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE*	CUI
AC-20(2)	*USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES*	CUI
AC-21	Information Sharing	FED
AC-22	Publicly Accessible Content	CUI

TABLE E-2: TAILORING ACTIONS FOR AWARENESS AND TRAINING CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
AT-1	Security Awareness and Training Policy and Procedures	NFO
AT-2	Security Awareness Training	CUI
AT-2(2)	*SECURITY AWARENESS	INSIDER THREAT*	CUI
AT-3	Role-Based Security Training	CUI
AT-4	Security Training Records	NFO

TABLE E-3: TAILORING ACTIONS FOR AUDITING AND ACCOUNTABILITY CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
AU-1	Audit and Accountability Policy and Procedures	NFO
AU-2	Audit Events	CUI
AU-2(3)	*AUDIT EVENTS | REVIEWS AND UPDATES*	CUI
AU-3	Content of Audit Records	CUI
AU-3(1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*	CUI
AU-4	Audit Storage Capacity	NCO
AU-5	Response to Audit Processing Failures	CUI
AU-6	Audit Review, Analysis, and Reporting	CUI
AU-6(1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*	NCO
AU-6(3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*	CUI
AU-7	Audit Reduction and Report Generation	CUI
AU-7(1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*	NCO
AU-8	Time Stamps	CUI
AU-8(1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*	CUI
AU-9	Protection of Audit Information	CUI
AU-9(4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*	CUI
AU-11	Audit Record Retention	NCO
AU-12	Audit Generation	CUI

TABLE E-4: TAILORING ACTIONS FOR SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CA-1	Security Assessment and Authorization Policies and Procedures	NFO
CA-2	Security Assessments	CUI
CA-2(1)	*SECURITY ASSESSMENTS* | *INDEPENDENT ASSESSORS*	NFO
CA-3	System Interconnections	NFO
CA-3(5)	*SYSTEM INTERCONNECTIONS* | *RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*	NFO
CA-5	Plan of Action and Milestones	CUI
CA-6	Security Authorization	FED
CA-7	Continuous Monitoring	CUI
CA-7(1)	*CONTINUOUS MONITORING* | *INDEPENDENT ASSESSMENT*	NFO
CA-9	Internal System Connections	NFO

TABLE E-5: TAILORING ACTIONS FOR CONFIGURATION MANAGEMENT CONTROLS [37]

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CM-1	Configuration Management Policy and Procedures	NFO
CM-2	Baseline Configuration	CUI
CM-2(1)	*BASELINE CONFIGURATION	REVIEWS AND UPDATES*	NFO
CM-2(3)	*BASELINE CONFIGURATION	RETENTION OF PREVIOUS CONFIGURATIONS*	NCO
CM-2(7)	*BASELINE CONFIGURATION	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*	NFO
CM-3	Configuration Change Control	CUI
CM-3(2)	*CONFIGURATION CHANGE CONTROL	TEST / VALIDATE / DOCUMENT CHANGES*	NFO
CM-4	Security Impact Analysis	CUI
CM-5	Access Restrictions for Change	CUI
CM-6	Configuration Settings	CUI
CM-7	Least Functionality	CUI
CM-7(1)	*LEAST FUNCTIONALITY	PERIODIC REVIEW*	CUI
CM-7(2)	*LEAST FUNCTIONALITY	PREVENT PROGRAM EXECUTION*	CUI
CM-7(4)(5)	*LEAST FUNCTIONALITY	UNAUTHORIZED OR AUTHORIZED SOFTWARE / BLACKLISTING OR WHITELISTING*	CUI
CM-8	System Component Inventory	CUI
CM-8(1)	*SYSTEM COMPONENT INVENTORY	UPDATES DURING INSTALLATIONS / REMOVALS*	CUI
CM-8(3)	*SYSTEM COMPONENT INVENTORY	AUTOMATED UNAUTHORIZED COMPONENT DETECTION*	NCO
CM-8(5)	*SYSTEM COMPONENT INVENTORY	NO DUPLICATE ACCOUNTING OF COMPONENTS*	NFO
CM-9	Configuration Management Plan	NFO
CM-10	Software Usage Restrictions	NCO
CM-11	User-Installed Software	CUI

[37] CM-7(5), Least Functionality *whitelisting*, is not in the moderate security control baseline in accordance with NIST Special Publication 800-53. However, it is offered as an optional and stronger policy alternative to *blacklisting*.

TABLE E-6: TAILORING ACTIONS FOR CONTINGENCY PLANNING CONTROLS[38]

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CP-1	Contingency Planning Policy and Procedures	NCO
CP-2	Contingency Plan	NCO
CP-2(1)	*CONTINGENCY PLAN	COORDINATE WITH RELATED PLANS*	NCO
CP-2(3)	*CONTINGENCY PLAN	RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	NCO
CP-2(8)	*CONTINGENCY PLAN	IDENTIFY CRITICAL ASSETS*	NCO
CP-3	Contingency Training	NCO
CP-4	Contingency Plan Testing	NCO
CP-4(1)	*CONTINGENCY PLAN TESTING	COORDINATE WITH RELATED PLANS*	NCO
CP-6	Alternate Storage Site	NCO
CP-6(1)	*ALTERNATE STORAGE SITE	SEPARATION FROM PRIMARY SITE*	NCO
CP-6(3)	*ALTERNATE STORAGE SITE	ACCESSIBILITY*	NCO
CP-7	Alternate Processing Site	NCO
CP-7(1)	*ALTERNATE PROCESSING SITE	SEPARATION FROM PRIMARY SITE*	NCO
CP-7(2)	*ALTERNATE PROCESSING SITE	ACCESSIBILITY*	NCO
CP-7(3)	*ALTERNATE PROCESSING SITE	PRIORITY OF SERVICE*	NCO
CP-8	Telecommunications Services	NCO
CP-8(1)	*TELECOMMUNICATIONS SERVICES	PRIORITY OF SERVICE PROVISIONS*	NCO
CP-8(2)	*TELECOMMUNICATIONS SERVICES	SINGLE POINTS OF FAILURE*	NCO
CP-9	System Backup	CUI
CP-9(1)	*SYSTEM BACKUP	TESTING FOR RELIABILITY / INTEGRITY*	NCO
CP-10	System Recovery and Reconstitution	NCO
CP-10(2)	*SYSTEM RECOVERY AND RECONSTITUTION	TRANSACTION RECOVERY*	NCO

[38] CP-9 is grouped with the security controls in the *Media Protection* family in Appendix D since the *Contingency Planning* family was not included in the security requirements.

TABLE E-7: TAILORING ACTIONS FOR IDENTIFICATION AND AUTHENTICATION CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
IA-1	Identification and Authentication Policy and Procedures	NFO
IA-2	Identification and Authentication (Organizational Users)	CUI
IA-2(1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*	CUI
IA-2(2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*	CUI
IA-2(3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*	CUI
IA-2(8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*	CUI
IA-2(9)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*	CUI
IA-2(11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*	FED
IA-2(12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS*	FED
IA-3	Device Identification and Authentication	CUI
IA-4	Identifier Management	CUI
IA-5	Authenticator Management	CUI
IA-5(1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*	CUI
IA-5(2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*	FED
IA-5(3)	*AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*	FED
IA-5(11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*	FED
IA-6	Authenticator Feedback	CUI
IA-7	Cryptographic Module Authentication	FED
IA-8	Identification and Authentication (Non-Organizational Users)	FED
IA-8(1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*	FED
IA-8(2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*	FED
IA-8(3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*	FED
IA-8(4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*	FED

TABLE E-8: TAILORING ACTIONS FOR INCIDENT RESPONSE CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
IR-1	Incident Response Policy and Procedures	NFO
IR-2	Incident Response Training	CUI
IR-3	Incident Response Testing	CUI
IR-3(2)	*INCIDENT RESPONSE TESTING	COORDINATION WITH RELATED PLANS*	NCO
IR-4	Incident Handling	CUI
IR-4(1)	*INCIDENT HANDLING	AUTOMATED INCIDENT HANDLING PROCESSES*	NCO
IR-5	Incident Monitoring	CUI
IR-6	Incident Reporting	CUI
IR-6(1)	*INCIDENT REPORTING	AUTOMATED REPORTING*	NCO
IR-7	Incident Response Assistance	CUI
IR-7(1)	*INCIDENT RESPONSE ASSISTANCE	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*	NCO
IR-8	Incident Response Plan	NFO

TABLE E-9: TAILORING ACTIONS FOR MAINTENANCE CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
MA-1	System Maintenance Policy and Procedures	NFO
MA-2	Controlled Maintenance	CUI
MA-3	Maintenance Tools	CUI
MA-3(1)	*MAINTENANCE TOOLS* | *INSPECT TOOLS*	CUI
MA-3(2)	*MAINTENANCE TOOLS* | *INSPECT MEDIA*	CUI
MA-4	Nonlocal Maintenance	CUI
MA-4(2)	*NONLOCAL MAINTENANCE* | *DOCUMENT NONLOCAL MAINTENANCE*	NFO
MA-5	Maintenance Personnel	CUI
MA-6	Timely Maintenance	NCO

TABLE E-10: TAILORING ACTIONS FOR MEDIA PROTECTION CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
MP-1	Media Protection Policy and Procedures	NFO
MP-2	Media Access	CUI
MP-3	Media Marking	CUI
MP-4	Media Storage	CUI
MP-5	Media Transport	CUI
MP-5(4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*	CUI
MP-6	Media Sanitization	CUI
MP-7	Media Use	CUI
MP-7(1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*	CUI

TABLE E-11: TAILORING ACTIONS FOR PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PE-1	Physical and Environmental Protection Policy and Procedures	NFO
PE-2	Physical Access Authorizations	CUI
PE-3	Physical Access Control	CUI
PE-4	Access Control for Transmission Medium	CUI
PE-5	Access Control for Output Devices	CUI
PE-6	Monitoring Physical Access	CUI
PE-6(1)	*MONITORING PHYSICAL ACCESS* | *INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*	NFO
PE-8	Visitor Access Records	NFO
PE-9	Power Equipment and Cabling	NCO
PE-10	Emergency Shutoff	NCO
PE-11	Emergency Power	NCO
PE-12	Emergency Lighting	NCO
PE-13	Fire Protection	NCO
PE-13(3)	*FIRE PROTECTION* | *AUTOMATIC FIRE SUPPRESSION*	NCO
PE-14	Temperature and Humidity Controls	NCO
PE-15	Water Damage Protection	NCO
PE-16	Delivery and Removal	NFO
PE-17	Alternate Work Site	CUI

TABLE E-12: TAILORING ACTIONS FOR PLANNING CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PL-1	Security Planning Policy and Procedures	NFO
PL-2	System Security Plan	CUI
PL-2(3)	*SYSTEM SECURITY PLAN	PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	NFO
PL-4	Rules of Behavior	NFO
PL-4(1)	*RULES OF BEHAVIOR	SOCIAL MEDIA AND NETWORKING RESTRICTIONS*	NFO
PL-8	Information Security Architecture	NFO

TABLE E-13: TAILORING ACTIONS FOR PERSONNEL SECURITY CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PS-1	Personnel Security Policy and Procedures	NFO
PS-2	Position Risk Designation	FED
PS-3	Personnel Screening	CUI
PS-4	Personnel Termination	CUI
PS-5	Personnel Transfer	CUI
PS-6	Access Agreements	NFO
PS-7	Third-Party Personnel Security	NFO
PS-8	Personnel Sanctions	NFO

TABLE E-14: TAILORING ACTIONS FOR RISK ASSESSMENT CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
RA-1	Risk Assessment Policy and Procedures	NFO
RA-2	Security Categorization	FED
RA-3	Risk Assessment	CUI
RA-5	Vulnerability Scanning	CUI
RA-5(1)	*VULNERABILITY SCANNING	UPDATE TOOL CAPABILITY*	NFO
RA-5(2)	*VULNERABILITY SCANNING	UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*	NFO
RA-5(5)	*VULNERABILITY SCANNING	PRIVILEGED ACCESS*	CUI

TABLE E-15: TAILORING ACTIONS FOR SYSTEM AND SERVICES ACQUISITION CONTROLS[39]

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
SA-1	System and Services Acquisition Policy and Procedures	NFO
SA-2	Allocation of Resources	NFO
SA-3	System Development Life Cycle	NFO
SA-4	Acquisition Process	NFO
SA-4(1)	*ACQUISITION PROCESS	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	NFO
SA-4(2)	*ACQUISITION PROCESS	DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*	NFO
SA-4(9)	*ACQUISITION PROCESS	FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*	NFO
SA-4(10)	*ACQUISITION PROCESS	USE OF APPROVED PIV PRODUCTS*	NFO
SA-5	System Documentation	NFO
SA-8	Security Engineering Principles	CUI
SA-9	External System Services	NFO
SA-9(2)	*EXTERNAL SYSTEMS	IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*	NFO
SA-10	Developer Configuration Management	NFO
SA-11	Developer Security Testing and Evaluation	NFO

[39] SA-8 is grouped with the security controls in the *System and Communications Protection* family in Appendix D since the *System and Services Acquisition* family was not included in the security requirements.

TABLE E-16: TAILORING ACTIONS FOR SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
SC-1	System and Communications Protection Policy and Procedures	NFO
SC-2	Application Partitioning	CUI
SC-4	Information in Shared Resources	CUI
SC-5	Denial of Service Protection	NCO
SC-7	Boundary Protection	CUI
SC-7(3)	*BOUNDARY PROTECTION | ACCESS POINTS*	NFO
SC-7(4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*	NFO
SC-7(5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*	CUI
SC-7(7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*	CUI
SC-8	Transmission Confidentiality and Integrity	CUI
SC-8(1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*	CUI
SC-10	Network Disconnect	CUI
SC-12	Cryptographic Key Establishment and Management	CUI
SC-13	Cryptographic Protection	CUI
SC-15	Collaborative Computing Devices	CUI
SC-17	Public Key Infrastructure Certificates	FED
SC-18	Mobile Code	CUI
SC-19	Voice over Internet Protocol	CUI
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	NFO
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	NFO
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NFO
SC-23	Session Authenticity	CUI
SC-28	Protection of Information at Rest	CUI
SC-39	Process Isolation	NFO

TABLE E-17: TAILORING ACTIONS FOR SYSTEM AND INFORMATION INTEGRITY CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
SI-1	System and Information Integrity Policy and Procedures	NFO
SI-2	Flaw Remediation	CUI
SI-2(2)	*FLAW REMEDIATION	AUTOMATED FLAW REMEDIATION STATUS*	NCO
SI-3	Malicious Code Protection	CUI
SI-3(1)	*MALICIOUS CODE PROTECTION	CENTRAL MANAGEMENT*	NCO
SI-3(2)	*MALICIOUS CODE PROTECTION	AUTOMATIC UPDATES*	NCO
SI-4	System Monitoring	CUI
SI-4(2)	*SYSTEM MONITORING	AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*	NCO
SI-4(4)	*SYSTEM MONITORING	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*	CUI
SI-4(5)	*SYSTEM MONITORING	SYSTEM-GENERATED ALERTS*	NFO
SI-5	Security Alerts, Advisories, and Directives	CUI
SI-7	Software, Firmware, and Information Integrity	NCO
SI-7(1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	INTEGRITY CHECKS*	NCO
SI-7(7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	INTEGRATION OF DETECTION AND RESPONSE*	NCO
SI-8	Spam Protection	NCO
SI-8(1)	*SPAM PROTECTION	CENTRAL MANAGEMENT*	NCO
SI-8(2)	*SPAM PROTECTION	AUTOMATIC UPDATES*	NCO
SI-10	Information Input Validation	NCO
SI-11	Error Handling	NCO
SI-12	Information Handling and Retention	FED
SI-16	Memory Protection	NFO