NIST Special Publication 800-171

Final Public Draft

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

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

NIST Special Publication 800-171

Final Public Draft

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
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 Office of the CIO
Department of Defense

April 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting 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. § 3541 *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, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

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
77 pages (April 2015)

CODEN: NSPUE2

draft

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. Computer Security Division publications are available at **http://csrc.nist.gov/publications**.

Public comment period: April 2 through May 12, 2015
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**

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) while residing in nonfederal information systems 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. This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI: (i) when the CUI is resident in nonfederal information systems and organizations; (ii) where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry; and (iii) when the information systems where the CUI resides are *not* operated by organizations on behalf of the federal government. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Draft

Keywords

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

Acknowledgements

The authors gratefully acknowledge and appreciate the contributions from Matt Barrett, Jon Boyens, Devin Casey, Jim Foti, Rich Graubart, Michael Nieles, Karen Quigg, 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.

Draft

Notes to Reviewers

The final draft of NIST Special Publication 800-171 contains some significant changes based on the comments received from both the public and private sectors. The changes include:

- Clarifying the purpose, scope, and applicability of the publication;
- Defining the underlying assumptions and expectations for federal agencies and nonfederal organizations in applying the recommended CUI security requirements;
- Explaining how the publication relates to the *Controlled Unclassified Information (CUI) federal rule* and the *Federal Acquisition Regulation (FAR) clause* to be sponsored by the National Archives and Records Administration (NARA);
- Adjusting the CUI security requirements to ensure complete coverage and traceability to federal policies, standards, and guidance;
- Providing tables that illustrate the mapping of CUI security requirements to security controls in NIST Special Publication 800-53 and ISO /IEC 27001;
- Providing tables that illustrate the tailoring actions on the NIST Special Publication 800-53 moderate security control baseline; and
- Adding guidance on using the content of the mapping tables to support implementation of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

The final publication of Special Publication 800-171 is targeted for June 2015 after the final public comment period. Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape our publications and ensure that they are meeting the needs and expectations of our customers.

-- Ron Ross
National Institute of Standards and Technology

Draft

Cautionary Note

The Federal Information Security Modernization Act (FISMA) 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: (i) information collected or maintained by or on behalf of an agency; or (ii) 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* information systems and organizations, and recommending security requirements to achieve that objective. It does not change, in any manner, 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 the Office of Management and Budget (OMB), and the supporting security standards and guidelines developed by the National Institute of Standards and Technology (NIST). See page viii, *When To Use Special Publication 800-171*.

The CUI 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 based on the proposed CUI rule (32 CFR Part 2002, *Controlled Unclassified Information*). The requirements and controls have been determined over time to provide the necessary protection for federal information and information systems that are covered under the Federal Information Security Modernization Act (FISMA). The tailoring criteria applied to the FIPS Publication 200 security requirements and the NIST Special Publication 800-53 security controls should ***not*** be interpreted as 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 information systems and organizations.

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. Organizations that are interested in or required to comply with the recommendations in this publications 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 range of cyber and kinetic threats to organizational missions and business operations. Addressing such threats is important because of the dependence many organizations have on their information technology infrastructures for 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 will issue a federal CUI rule in 2015 to establish the required controls and markings for CUI governmentwide. This rule, 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 rule 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 rule will not create these policies, standards, and guidelines which are already established by OMB and NIST. Rather, the rule will require adherence to the policies and use of the standards and guidelines in the same way 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 — defining security requirements for protecting CUI in nonfederal information systems and organizations. This 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 be in compliance 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 2016, a single Federal Acquisition Regulation (FAR) clause that will apply the requirements of the federal CUI rule and NIST 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. Until the formal process of establishing such a single FAR clause takes place, the CUI requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

When To Use Special Publication 800-171

Special Publication 800-171 is intended for use by federal agencies when agencies are providing CUI to nonfederal organizations (or when CUI is developed by those organizations for federal agencies) for purposes unrelated to information processing—that is, the nonfederal organizations are not operating their information systems to process agency data, including CUI, on behalf of the agency but rather for other purposes (e.g., when designing or producing an aircraft, performing a study, or conducting background investigations for security clearances). Nonfederal organizations typically employ their internal information system resources to develop the required deliverables associated with specific federal contracts or other agreements with the federal government. The nonfederal organization's information system will also be required to process, store, transmit, or generate any CUI needed to develop those deliverables. In such cases, the requirements in Special Publication 800-171 are applied, recognizing that nonfederal organizations: (i) must meet their internal organizational information processing needs; and (ii) may also be required to support the information processing needs of other organizations.

In situations where federal agencies provide CUI to nonfederal organizations for processing on their behalf (e.g., information processing centers, data centers), agencies should generally apply the suite of federal standards and guidelines (including FIPS Publication 199, FIPS Publication 200, Special Publication 800-53, and Special Publication 800-60) to those information systems. Since the CUI is being *processed on behalf of the federal agency* by the nonfederal organization, the system would be considered a federal information system under FISMA. The use of Special Publication 800-171 would be inappropriate since it does not include any availability requirements or controls that should be part of an information system processing service, such as cloud-based services. See *Cautionary Note* on page vi of this publication for specific FISMA applicability criteria.

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. Once identified, those controls can be located in 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 CUI 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. See www.nist.gov/cyberframework.

Draft

Table of Contents

CHAPTER ONE INTRODUCTION 1
1.1 PURPOSE AND APPLICABILITY 2
1.2 TARGET AUDIENCE 3
1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION 4
CHAPTER TWO THE FUNDAMENTALS 5
2.1 BASIC ASSUMPTIONS 5
2.2 DEVELOPMENT OF CUI REQUIREMENTS 6
CHAPTER THREE THE REQUIREMENTS 8
3.1 ACCESS CONTROL 9
3.2 AWARENESS AND TRAINING 9
3.3 AUDIT AND ACCOUNTABILITY 10
3.4 CONFIGURATION MANAGEMENT 10
3.5 IDENTIFICATION AND AUTHENTICATION 11
3.6 INCIDENT RESPONSE 11
3.7 MAINTENANCE 12
3.8 MEDIA PROTECTION 12
3.10 PHYSICAL PROTECTION 13
3.11 RISK ASSESSMENT 13
3.12 SECURITY ASSESSMENT 13
3.13 SYSTEM AND COMMUNICATIONS PROTECTION 13
3.14 SYSTEM AND INFORMATION INTEGRITY 14
APPENDIX A REFERENCES A-1
APPENDIX B GLOSSARY B-1
APPENDIX C ACRONYMS C-1
APPENDIX D MAPPING TABLES D-1
APPENDIX E TAILORING CRITERIA E-1

Draft

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. Many federal contractors, for example, routinely process, store, and transmit sensitive federal information in their information systems[1] 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 information 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 information 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*.[3] The Executive Order established a governmentwide Controlled Unclassified Information (CUI) Program[4] 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[5] 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*.[6] The CUI Registry is the online repository for information, guidance, policy, and

[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 such as industrial/process controls systems.

[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. An information system that does not meet such criteria is a *nonfederal information system*.

[3] See www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information.

[4] *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.

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

[6] See www.archives.gov/cui/registry/category-list.html.

requirements on handling CUI, including issuances by the CUI Executive Agent. Among other information, the CUI Registry identifies approved CUI categories and subcategories, provides 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, re-using, 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 *rule*,[7] 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 requirements for protecting the *confidentiality* of CUI: (i) when the CUI is resident in nonfederal information systems and organizations; (ii) where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the Registry; and (iii) when the information systems where the CUI resides are *not* operated by organizations on behalf of the federal government. The requirements apply *only* to components[8] of nonfederal information systems that process, store, or transmit CUI, or provide security protection for such components. The CUI 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 associated CUI Federal Acquisition Regulation (FAR),[9] the CUI Executive Agent will address determining compliance with CUI requirements in nonfederal organizations. Determining compliance is *not* within the scope of this publication.

In accordance with the federal CUI rule, federal information systems and organizations that 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 impact)[10]

[7] Proposed 32 CFR Part 2002, *Controlled Unclassified Information*, projected for publication in 2015.

[8] Information system *components* include, for example: mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name); input/output devices (e.g., scanners, copiers, printers, tablets, smartphones); network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors); operating systems; virtual machines; and applications.

[9] NARA, in its capacity as the CUI Executive Agent, plans to sponsor in 2016, a single FAR clause that will apply the requirements of the federal CUI rule and NIST Special Publication 800-171 to contractors. Until the formal process of establishing such a single FAR clause takes place, the CUI requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

[10] 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*.[11]

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 information systems.[12] The specific requirements for safeguarding CUI in nonfederal information 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 rule is limited to the security objective of confidentiality (i.e., not directly addressing integrity and availability) and that some of the FISMA-related 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 rule. Rather, the intent is to express the requirements in a manner that allows for and facilitates the equivalent safeguarding measures within nonfederal information systems and organizations and does not diminish the level of protection of CUI required for moderate confidentiality.

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 information system development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, information system/security engineers, systems integrators);
- Individuals with acquisition or procurement responsibilities (e.g., contracting officers);
- Individuals with information system, security, and/or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, information system owners, information security managers); and
- Individuals with information 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: (i) the *federal perspective* as the entity establishing and conveying the CUI security requirements in contractual vehicles or other types of inter-organizational agreements; and (ii) the *nonfederal perspective* as the entity responding to and complying with the CUI security requirements set forth in contracts or agreements.

[11] NIST Special Publication 800-60 will be updated to ensure consistency with the CUI Registry. The CUI Registry (i) identifies all of the approved categories and subcategories of CUI; (ii) provides general descriptions for each category and subcategory; and (iii) identifies the basis for safeguarding and dissemination controls.

[12] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal information system. Examples of nonfederal organizations include State and local governments, colleges and universities, and contractors.

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the assumptions and methodology used to develop the CUI security requirements, 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 information systems and organizations.
- **Supporting appendices** provide additional information related to the protection of CUI in nonfederal information systems and organizations including: (i) general references; (ii) a glossary of definitions and terms; (iii) acronyms used in this publication; (iv) mapping tables relating the CUI security requirements to the security controls in NIST Special Publication 800-53 and ISO/IEC 27001; and (v) an explanation of the tailoring actions employed on the moderate security control baseline.

Draft

CHAPTER TWO

THE FUNDAMENTALS

ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING CUI SECURITY REQUIREMENTS

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

2.1 BASIC ASSUMPTIONS

The CUI 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 information systems or nonfederal information systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal information systems and organizations; and
- The confidentiality impact value for CUI is no lower than *moderate*[13] in accordance with Federal Information Processing Standards (FIPS) Publication 199.[14]

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 CUI 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 information 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 CUI security requirements;
- Nonfederal organizations can implement a variety of potential security solutions either directly or through the use of managed services, to satisfy CUI security requirements; and
- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every CUI security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.

[13] 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.

[14] In accordance with proposed 32 CFR Part 2002, *Controlled Unclassified Information*, there will be only one level of safeguarding for CUI (i.e., moderate impact for confidentiality) unless federal law, regulation, or governmentwide policy specifies otherwise.

2.2 DEVELOPMENT OF CUI REQUIREMENTS

Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of: (i) a *basic security requirements* section; and (ii) 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 information 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 information 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.[15]

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 information systems and organizations. Appendix D provides informal mappings of the CUI security requirements to the relevant security controls in NIST Special Publication 800-53 and ISO/IEC 27001. The mappings are included to promote a better understanding of the CUI 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 CUI security requirement:

<u>Basic Security Requirements</u>:

- Establish and maintain baseline configurations and inventories of organizational information 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 information systems.

<u>Derived Security Requirements</u>:

- Track, review, approve/disapprove, and audit changes to information systems.
- Analyze the security impact of changes prior to implementation.

[15] The CUI 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 necessary for a *comprehensive* information security program. The strength and quality of such programs in nonfederal organizations depends 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 CUI requirements in Chapter Three.

- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- Employ the principle of least functionality by configuring the information system 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 information 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.[16] 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

[16] Two exceptions include: (i) a requirement to protect the confidentiality of system backups (derived from CP-9) from the *contingency planning* family; and (ii) 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* 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)[17] for protecting the confidentiality of CUI in nonfederal information 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 CUI 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 CUI requirements if needed).[20] This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk.

Cost-Effective and Efficient Implementation of CUI Requirements

If the nonfederal organization entrusted with protecting CUI designates specific information systems or components of systems for the processing, storage, or transmission of CUI, then the organization may limit the scope of this publication's security requirements to those particular systems or components. Isolating CUI into its own security domain by applying architectural design principles may be the most cost-effective and efficient way for a nonfederal organization to satisfy the security requirements and protect the confidentiality of CUI. This approach can: (i) reasonably provide adequate security for the CUI; and (ii) avoid increasing the organization's security posture to a level beyond which it typically requires for protecting its core business operations and assets. Nonfederal organizations may choose to use the same CUI infrastructure for multiple government contracts, as long as the CUI has the same safeguarding requirements (i.e., the CUI does not have specific safeguarding required or permitted by the authorizing law, regulation, or governmentwide policy).

[17] The security requirements identified in this publication are intended to be applied to the nonfederal organization's general purpose internal information systems that are processing, storing, or transmitting CUI. Some specialized systems such as medical devices, Computer Numerical Control (CNC) machines, or industrial control systems may have restrictions or limitations on the application of certain CUI requirements and may be granted waivers or exemptions from the requirements by the federal agency providing oversight.

[18] 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 information system level support both security objectives. Thus, the integrity requirements (either basic or derived) 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 CUI 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] Additional CUI security requirements beyond those requirements described in this publication may be justified *only* when such requirements are based on federal law, regulation, or governmentwide policy and indicated in the CUI Registry as *CUI specified*. The provision of safeguarding requirements for CUI in a particular 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.

3.1 ACCESS CONTROL

Basic Security Requirements:

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

3.1.2 Limit information 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/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.

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

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

3.1.22 Control information posted or processed on publicly accessible information systems.

3.2 AWARENESS AND TRAINING

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information 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 organizational information systems.

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

Draft

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

3.3.2 Ensure that the actions of individual information 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 Use automated mechanisms to integrate and 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 an information 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.

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information 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 information systems.

Derived Security Requirements:

3.4.3 Track, review, approve/disapprove, and audit changes to information 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 the information system.

3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.

3.4.7 Restrict, disable, and 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.

Draft

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements:

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

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

Derived Security Requirements:

3.5.3 Use multifactor authentication[21] for local and network access[22] 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.

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 encrypted representation of 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 information systems that includes adequate 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.

Draft

[21] *Multifactor authentication* requires two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) 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.

[22] *Local access* is any access to an information 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 an information 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).

3.7 MAINTENANCE

Basic Security Requirements:

3.7.1 Perform maintenance on organizational information systems.[23]

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

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) information system media containing CUI, both paper and digital.

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

3.8.3 Sanitize or destroy information 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.

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 information 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 information systems containing CUI.

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

Derived Security Requirements: None.

[23] 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.

Draft

3.10 PHYSICAL PROTECTION

Basic Security Requirements:

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

3.10.2 Protect and monitor the physical facility and support infrastructure for those information 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 (e.g., telework 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 information systems and the associated processing, storage, or transmission of CUI.

Derived Security Requirements:

3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system 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 information 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 information systems.

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

Derived Security Requirements: None.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements:

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

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

Derived Security Requirements:

3.13.3 Separate user functionality from information system management functionality.

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

Draft

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 the information system and communicating via some other connection to resources in external networks.

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

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 the information system;

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

3.13.12 Prohibit remote activation 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 information and information system flaws in a timely manner.

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

3.14.3 Monitor information system security alerts and advisories and take appropriate actions 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 the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7 Identify unauthorized use of the information system.

Draft

NARA, CUI 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. Regarding contractors, the CUI Executive Agent anticipates establishing a single Federal Acquisition Regulation (FAR) clause in 2016 to apply the requirements of NIST Special Publication 800-171 to the contractor environment as well as to determine oversight responsibilities and requirements. The CUI Executive Agent also addresses its oversight of federal agencies in the proposed rule for incorporation into the Code of Federal Regulations. Approaches to oversight will be determined through the uniform CUI FAR clause, future understandings, and agreements between federal agencies and their nonfederal information sharing partners.

Draft

APPENDIX A

REFERENCES

LAWS, EXECUTIVE ORDERS, POLICIES, REGULATIONS, STANDARDS, AND GUIDELINES

LEGISLATION, EXECUTIVE ORDERS, REGULATIONS, AND POLICIES

1. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014.
2. Executive Order 13556, *Controlled Unclassified Information*, November 2010.
3. 32 CFR Part 2002, *Controlled Unclassified Information*, Public Draft 2015.

STANDARDS AND GUIDELINES

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
3. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
4. National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, December 2014.
5. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 1, August 2008.
6. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 2, August 2008.
7. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 2014.

Draft

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 [CNSSI 4009]	A chronological record of information 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]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information 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 an information 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	The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) 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 information 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 information system.

Draft

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	Those types of information for which law, regulation, or governmentwide policy requires safeguarding or disseminating controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.
CUI Executive Agent	The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
CUI Program	The executive branch-wide program to standardize CUI handling by 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	The online repository for all information, guidance, policy, and requirements on handling CUI, including all issuances by the CUI Executive Agent. Among other information, the CUI Registry identifies approved CUI categories and subcategories, provides 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, re-using, and disposing of the information.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information 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 Information System (or Component)	An information system or component of an information 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 Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information 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.

Draft

External Information System Service Provider	A provider of external information 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 [CNSSI 4009]	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 [CNSSI 4009]	The physical components of an information system. See *Software* and *Firmware*.
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 an information 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]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information 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 [CNSSI 4009]	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 Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.

Draft

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 System Component [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission.
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.
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: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
Local Access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Draft

Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information 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 an information system.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing 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: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See *Authenticator*.
Nonfederal Information System	An information system that does not meet the criteria for a federal information system.
Nonfederal Organization	An entity that owns, operates, or maintains a nonfederal information system.
Network [CNSSI 4009]	Information system(s) 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 an information 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.

Draft

Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure.
Portable Storage Device	An information system component that can be inserted into and removed from an information 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	An information system account with authorizations of a privileged user.
Privileged User [CNSSI 4009]	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 information 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 information 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).
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. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Draft

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 an information 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 [CNSSI 4009]	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 information 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 an information 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 an information system or organization.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
System	See *Information System*.

Draft

Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information 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 an information system.
Whitelisting	The process used to identify: (i) software programs that are authorized to execute on an information system; or (ii) authorized Universal Resource Locators (URL)/websites.

Draft

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

Draft

APPENDIX D

MAPPING TABLES

MAPPING CUI SECURITY REQUIREMENTS TO SECURITY CONTROLS

Tables D-1 through D-14 provide an informal mapping of the CUI 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 CUI 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 CUI 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 CUI 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 CUI 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.

Draft

Table D-1: Mapping Access Control Requirements to Security Controls

CUI 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 information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information 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
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
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/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.*	
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.*	

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
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.	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 information systems.	AC-20	Use of External Information 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 Information Systems *Limits on Authorized Use*	*No direct mapping.*	
3.1.21 Limit use of organizational portable storage devices on external information systems.	AC-20(2)	Use of External Information Systems *Portable Storage Devices*	*No direct mapping.*	
3.1.22 Control information posted or processed on publicly accessible information systems.	AC-22	Publicly Accessible Content	*No direct mapping.*	

Table D-2: Mapping Awareness and Training Requirements to Security Controls

CUI 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 manager, systems administrators, and users of organizational information 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 organizational information systems. **3.2.2** Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
			A.12.2.1	Controls against malware
	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 Security Controls

CUI 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, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. **3.3.2** Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	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.*	
	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-12	Audit Generation	A.12.4.1	Event logging
			A.12.4.3	Administrator and operator logs
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 Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(1)	Audit Review, Analysis, and Reporting *Process Integration*	*No direct mapping.*	
	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 an information 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 synchronisation
	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

CUI 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.*

Draft

Table D-4: Mapping Configuration Management Requirements to Security Controls[24]

CUI 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 information 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 information systems.	CM-2	Baseline Configuration	*No direct mapping.*	
	CM-6	Configuration Settings	*No direct mapping.*	
	CM-8	Information System Component Inventory	A.8.1.1	Inventory of assets
			A.8.1.2	Ownership of assets
	CM-8(1)	Information System Component Inventory *Updates During Installations / Removals*	*No direct mapping.*	
Derived Security Requirements				
3.4.3 Track, review, approve/disapprove, and audit changes to information 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 the information system.	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

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

CUI 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 the information system to provide only essential capabilities.	CM-7	Least Functionality	A.12.5.1*	Installation of software on operational systems
3.4.7 Restrict, disable, and prevent the use of nonessential 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 Security Controls[25]

CUI 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 information system users, processes acting on behalf of users, or devices. **3.5.2** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
	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.*	
3.5.5 Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration

[25] 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 information systems transmitting CUI.

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
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.	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 encrypted representation of passwords.				
3.5.11	Obscure feedback of authentication information.	IA-6	Authenticator Feedback	A.9.4.2	Secure log-on procedures

Draft

Table D-6: Mapping Incident Response Requirements to Security Controls

CUI 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 information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. **3.6.2** Track, document, and report incidents to appropriate organizational officials and/or authorities.	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.*	
	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.*	
	IR-3(2)	Incident Response Testing *Coordination with Related Plans*	*No direct mapping.*	

Table D-7: Mapping Maintenance Requirements to Security Controls

CUI 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 information systems. **3.7.2** Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
			A.11.2.5*	Removal of assets
	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 the information system.			*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 Security Controls[26]

CUI 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) information system media containing CUI, both paper and digital. **3.8.2** Limit access to CUI on information system media to authorized users. **3.8.3** Sanitize or destroy information system media containing CUI before disposal or release for reuse.	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
	MP-4	Media Storage	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
	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 information 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 information system components.	MP-7	Media Use	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media

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

CUI 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	Information System Backup	A.12.3.1	Information backup
				A.17.1.2	Implementing information security continuity
				A.18.1.3	Protection of records

Draft

Table D-9: Mapping Personnel Security Requirements to Security Controls

CUI 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 information systems containing CUI. **3.9.2** Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	PS-3	Personnel Screening	A.7.1.1	Screening
	PS-4	Personnel Termination	A.7.3.1	Termination or change of employment responsibilities
			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.			

Draft

Table D-10: Mapping Physical Protection Requirements to Security Controls

CUI 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 information systems, equipment, and the respective operating environments to authorized individuals. **3.10.2** Protect and monitor the physical facility and support infrastructure for those information systems.	PE-2	Physical Access Authorizations	A.11.1.2*	Physical entry controls
	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 (e.g., telework 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 Security Controls

CUI 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 information 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 the information system and applications periodically and when new vulnerabilities affecting the system 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 Security Controls

CUI 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 information 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 information systems. **3.12.3** Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	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
	CA-5	Plan of Action and Milestones	*No direct mapping.*	
	CA-7	Continuous Monitoring	*No direct mapping.*	
Derived Security Requirements	None.			

Table D-13: Mapping System and Communications Protection Requirements to Security Controls[27]

CUI 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 organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information 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 information systems.	SA-8	Security Engineering Principles	A.14.2.5	Secure system engineering principles
Derived Security Requirements				
3.13.3 Separate user functionality from information system management functionality (e.g., privileged user functions).	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.*	

[27] 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 CUI security requirements.

CUI 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 the information system and communicating via some other connection to resources in external networks.	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 the information system.	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

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13.13	Manage the use of mobile code.	SC-18	Mobile Code	*No direct mapping.*	
3.13.14	Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies and monitor/control use of VoIP.	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

Draft

Table D-14: Mapping System and Information Integrity Requirements to Security Controls

CUI 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 information and information system flaws in a timely manner. **3.14.2** Provide protection from malicious code at appropriate locations within organizational information systems. **3.14.3** Monitor information system security alerts and advisories and take appropriate actions 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 the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.				
3.14.6 Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4	Information System Monitoring	*No direct mapping.*	
	SI-4(4)	Information System Monitoring *Inbound and Outbound Communications Traffic*	*No direct mapping.*	
3.14.7 Identify unauthorized use of the information system.	SI-4	Information 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 final CUI 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.[28] 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.[29]

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; or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.

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.

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

[29] 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.

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 Information Systems	CUI
AC-20(1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*	CUI
AC-20(2)	*USE OF EXTERNAL INFORMATION 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

Draft

Table E-3: Tailoring Actions for Audit 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*	CUI
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

Draft

Table E-5: Tailoring Actions for Configuration Management Controls[30]

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	Information System Component Inventory	CUI
CM-8(1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*	NFO
CM-8(3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*	NCO
CM-8(5)	*INFORMATION 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

[30] 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[31]

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	Information System Backup	CUI
CP-9(1)	*INFORMATION SYSTEM BACKUP	TESTING FOR RELIABILITY / INTEGRITY*	NCO
CP-10	Information System Recovery and Reconstitution	NCO
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	TRANSACTION RECOVERY*	NCO

[31] 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 CUI 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	NCO
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-2(1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*	NFO
IR-3	Incident Response Testing	CUI
IR-3(2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*	CUI
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

Draft

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

Draft

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

Draft

Table E11: 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	NFO
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	NFO
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

Draft

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

Draft

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

Draft

Table E-15: Tailoring Actions for System and Services Acquisition Controls[32]

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	Information System Documentation	NFO
SA-8	Security Engineering Principles	CUI
SA-9	External Information System Services	NFO
SA-9(2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*	NFO
SA-10	Developer Configuration Management	NFO
SA-11	Developer Security Testing and Evaluation	NFO

[32] 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 CUI 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	Information System Monitoring	CUI
SI-4(2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*	NCO
SI-4(4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*	CUI
SI-4(5)	*INFORMATION 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