The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-171**

Title: **Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**

Publication Date: **6/18/2015**

- Final Publication: https://doi.org/10.6028/NIST.SP.800-171 (which links to http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171.pdf).
- Related Information:
  - http://csrc.nist.gov/publications/PubsSPs.html#SP-800-171
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Nov. 18, 2014

SP 800-171

DRAFT Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

NIST announces the release of Draft Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (Initial Public Draft).

The protection of sensitive unclassified federal information while residing in nonfederal information systems and environments of operation is of paramount importance to federal agencies. Compromises of this information 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 Controlled Unclassified Information (CUI) as defined by Executive Order 13556, when such information resides in nonfederal information systems and organizations. The requirements apply to:

- Nonfederal information systems that are beyond the scope of the systems covered by the Federal Information Security Management Act (FISMA); and
- All components of nonfederal systems that process, store, or transmit CUI.

The CUI protection requirements were obtained from the security requirements and controls in FIPS Publication 200 and NIST SP 800-53, and then tailored appropriately to eliminate requirements that are:

- Primarily the responsibility of the federal government (i.e., uniquely federal);
- Related primarily to availability; or
- Assumed to be routinely satisfied by nonfederal organizations without any further specification.

Nonfederal organizations include, for example: federal contractors; state, local, and tribal governments; and colleges and universities.

This publication is part of a larger initiative by the National Archives and Records Administration (NARA) to fulfill their responsibilities as Executive Agent for Executive Order 13556 for CUI. NARA has a three-part plan to help standardize the naming conventions and protection requirements for sensitive information (designated CUI) both within the federal government and when such information resides in nonfederal information systems and organizations. NARA's plan includes:

- Incorporating uniform CUI policies and practices into the Code of Federal Regulations;
- Using NIST SP 800-171 to define requirements to protect the confidentiality of CUI; and
- Developing a standard Federal Acquisition Regulation (FAR) clause to levy the SP 800-171 security requirements to contractor environments.

Please send comments to sec-cert_@ nist.gov with "Comments Draft SP 800-171" in the subject line. Comments will be accepted through ***January 16, 2015***.

NIST Special Publication 800-171

Initial 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

Initial 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

November 2014

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 Management Act (FISMA), Public Law (P.L.) 107-347. 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
34 pages (November 2014)

CODEN: NSPUE2

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: November 18, 2014 through January 16, 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 sensitive unclassified federal information while residing in nonfederal information systems and environments of operation 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 Controlled Unclassified Information (CUI) as defined by Executive Order 13556, when such information resides in nonfederal information systems and organizations. The requirements apply to: (i) nonfederal information systems that are beyond the scope of the systems covered by the Federal Information Security Management Act (FISMA); and (ii) all components of nonfederal systems that process, store, or transmit CUI.

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 significant contributions from Jon Boyens, Rich Graubart, Murugiah Souppaya, and Jim Foti, 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.

Notes to Reviewers

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.[Note 1] Consistent with this tasking, and with the CUI Program's mission to establish uniform policies and practices across the federal government, NARA is issuing a Federal regulation, or directive, to establish the required controls and markings governmentwide. A regulation binds agencies throughout the Executive branch to uniformly apply the Program's standard safeguards, markings, dissemination, and decontrol requirements. The proposed rule, currently under Office of Management and Budget (OMB) coordination, contains a system of requirements that NARA developed in consultation with affected stakeholders, including nonfederal partners.

With regard to information systems, requirements for protection of CUI at the moderate confidentiality impact level in the proposed rule are based on applicable governmentwide standards and guidelines issued by NIST, and applicable policies established by OMB. The proposed rule does not create these standards, which are already established by OMB and NIST.[Note 2] Rather, the proposed rule requires the use of these standards in the same way throughout the Executive branch, thereby reducing current complexity for federal agencies and their nonfederal information-sharing partners, including contractors.

NARA has taken steps to alleviate the potential impact of the information security requirements on nonfederal organizations by jointly developing NIST Special Publication 800-171—thus, applying information security requirements, but based in the *nonfederal environment*. Doing so should make it easier for nonfederal organizations to comply with the standards using the systems they already have in place, rather than trying to use government-specific approaches.

The CUI Executive Agent also anticipates establishing a single *Federal Acquisition Regulation (FAR)* clause that will apply the requirements of the proposed rule and NIST Special Publication 800-171 to the contractor environment. This will further promote standardization to benefit a substantial number of nonfederal organizations that may struggle to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from different 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, where necessitated by exigent circumstances, NIST Special Publication 800-171 may be referenced in a contract-specific requirement on a limited basis consistent with the regulatory requirements.

To summarize, in the process of this three-part plan (i.e., development of the CUI rule, NIST Special Publication, and standard FAR clause), nonfederal organizations, including contractors, will not only receive streamlined and uniform requirements for all CUI security needs, but also will have information security requirements for CUI tailored to nonfederal systems, allowing the nonfederal organizations to be in compliance with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI.

Note 1: Executive Order 13556, Section 4b.

Note 2: The Order, in fact, states, "This order shall be implemented in a manner consistent with…applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget." (6a3)

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.

Establishing Expectations for this Publication

This publication recognizes that—

- The security requirements contained herein, *only* apply to nonfederal information systems (or components of nonfederal systems) and organizations that process, store, or transmit *Controlled Unclassified Information (CUI)* as defined by *Executive Order 13556*.
- Nonfederal organizations are not developing or acquiring new information systems specifically for the purpose of processing, storing, or transmitting CUI—rather, these organizations already have an information technology infrastructure, acquisition process, and associated security policies, procedures, and practices in place. Thus, federal information security requirements from *FIPS Publication 200* and associated security controls from *NIST Special Publication 800-53* in the Contingency Planning (CP) family, Planning (PL) family, System and Services Acquisition (SA) family, and Physical and Environmental Protection (PE) family (only requirements related to the environment in which the nonfederal system operates) have been deemed out of scope for this publication. Policy- and procedure-related requirements and controls from the above publications have also been eliminated from consideration. There are some exceptions where protecting CUI from disclosure may require some additional policies, procedures, and/or technologies that are beyond the standard practices one would anticipate finding in such organizations.
- Nonfederal organizations and their information systems may handle more than just federal information (e.g., CUI) and that there could be other constraints levied on those systems.
- There are many potential security solutions that can be implemented by nonfederal organizations to satisfy the security requirements—that is, alternative, but arguably *equivalent methods* may be employed.
- Nonfederal organizations may not always have the necessary organizational structure, resources, or infrastructure to satisfy every security requirement. For example, very small businesses or contractors may have difficulty in satisfying the separation of duty requirement. Federal agencies may consider such factors in their risk-based decisions and nonfederal organizations may in those situations, propose alternative security requirements that can compensate for the inability to satisfy a particular requirement.

Table of Contents

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 information system service providers[1] to help carry out a wide range of federal missions and business functions. Federal contractors, for example, routinely process, store, and transmit sensitive, unclassified federal information in their information systems to support the delivery of essential products and services to their federal customers (e.g., conducting basic or applied scientific research; conducting background investigations for security clearances; providing credit card and other financial services; providing Web support and electronic mail services; and developing healthcare, communications, and weapons systems). The protection of sensitive, unclassified federal information while residing in *nonfederal information systems*[2] and environments of operation is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions/business operations.

The protection of sensitive, unclassified federal information in nonfederal information systems and organizations is dependent on the federal government providing a disciplined and structured process for identifying the many different information/data types that are routinely used by federal agencies. On November 4, 2010, the President signed Executive Order 13556, *Controlled Unclassified Information* (the Order). The Order designated the National Archives and Records Administration (NARA) as the Executive Agent for Controlled Unclassified Information (CUI)[3] and directed NARA to implement a governmentwide CUI Program to standardize the way the Executive branch handles unclassified information that requires protection.[4] Only information that requires safeguarding or dissemination controls pursuant to law, federal regulations, and governmentwide policies 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*.[5] The CUI Registry: (i) identifies the exclusive categories and subcategories of unclassified information that require safeguarding and dissemination controls consistent with law, federal regulation, and governmentwide policies; and (ii) serves as the central repository for the posting of and access to the categories and subcategories, associated markings, and applicable

[1] An *external information system service provider* is a provider of 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.

[2] The Federal Information Security Management Act (FISMA) defines a federal information system as 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] *Controlled Unclassified Information* is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and governmentwide policies, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

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

[5] http://www.archives.gov/cui/registry/category-list.html.

safeguarding, dissemination, and decontrol procedures. The CUI Registry also includes the appropriate citation(s) of law, regulation, and/or governmentwide policy that form the basis for each category and subcategory.

The Order 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*,[6] developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI, self-inspection and oversight requirements, and 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 when such information resides in nonfederal information systems and organizations.[7] The security requirements apply only to components[8] of nonfederal information systems that process, store, or transmit CUI. In accordance with the CUI rule issued by NARA,[9] federal information systems 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 impact value for confidentiality);[10]
- Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (moderate baseline as tailored by the implementing organization); and
- NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.[11]

[6] Proposed 32 CFR Part 2002, *Controlled Unclassified Information*.

[7] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal information system.

[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), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, and applications.

[9] As set forth in Executive Order 13556, NARA as the Executive Agent for CUI, established minimum requirements for safeguarding such information.

[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. A serious adverse effect means that, for example, the loss of confidentiality might: (i) cause a significant degradation in mission or business capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

[11] The *information types* in NIST SP 800-60 are being updated to ensure consistency with the CUI categories and subcategories of unclassified information that have been defined by NARA in the CUI Registry.

The requirements for protecting the confidentiality of CUI in nonfederal information systems have been derived from the above authoritative publications using the design criteria described in Chapter 2.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience including:

- Individuals with information system development life cycle responsibilities (e.g., program managers, information owners/stewards, mission/business owners, information system owners, acquisition/procurement officials);
- 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 managers, information security managers); and
- Individuals with information security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

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 in developing the security requirements to protect the confidentiality of CUI in nonfederal information systems and organizations and options that can be employed by nonfederal organizations to determine compliance to such 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) definitions and terms; and (iii) acronyms.

CHAPTER TWO

THE FUNDAMENTALS

ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING CUI SECURITY REQUIREMENTS

This chapter: (i) describes the assumptions and methodology used in developing the security requirements to protect CUI in nonfederal information systems and organizations; and (ii) discusses the potential assessment options that can be employed to determine compliance to the CUI security requirements.

2.1 CONSTRUCTION OF CUI SECURITY REQUIREMENTS

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

- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal information systems or nonfederal information systems including the environments in which those systems operate;
- Safeguards or countermeasures implemented to protect CUI are *consistent* in both federal and nonfederal environments; and
- The confidentiality impact value for CUI is no lower than *moderate* in accordance with Federal Information Processing Standards (FIPS) Publication 199.[12]

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 agency or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies.

Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of the following: (i) a *basic security requirement* section; (ii) a *derived security requirements* section; and (iii) a *reference* section. The basic security requirements are obtained from FIPS Publication 200 and *tailored* appropriately to eliminate requirements that are:

- Primarily the responsibility of the federal government (i.e., uniquely federal);
- Related primarily to availability; or
- Assumed to be routinely satisfied by nonfederal organizations without any further specification.

The derived security requirements, which supplement the basic security requirements, are taken from the security control language in NIST Special Publication 800-53. Starting with the moderate security control baseline (i.e., the minimum level of protection for CUI in federal information systems), the SP 800-53 controls are *tailored* using the same criteria used to tailor the FIPS 200 requirements. After tailoring the moderate baseline to eliminate security controls that are uniquely federal, availability-related, and assumed to be routinely satisfied by nonfederal

[12] Proposed 32 CFR Part 2002, *Controlled Unclassified Information*. Additional security requirements may be required by a federal agency only internally, but must not be required for any safeguarding external to the agency, including contractors when not processing on behalf of an agency.

organizations without further specification, the remaining control language (*not* already included in the basic security requirement) forms the basis of the derived security requirements. The combination of the basic and derived security requirements captures the intent of FIPS 200 and SP 800-53, with respect to the protection of the *confidentiality* of CUI in nonfederal information systems and organizations.

Finally, the references section includes a listing of the security controls from SP 800-53 that provides the basis, along with FIPS 200, for the security requirements. The security control references are included to provide additional reference material to nonfederal organizations to promote a better understanding of the 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.

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

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

Derived Security Requirements:

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

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

c. Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services; and

d. Apply deny by exception (blacklist) policy to prevent the use of unauthorized software.

References: NIST Special Publication 800-53.

CONFIGURATION MANAGEMENT	CM-2; CM-4; CM-5; CM-6; CM-7; CM-7(1); CM-7(2); CM-7(4); CM-8.

For ease of use, the security requirements are organized into fourteen *families*.[13] Each family contains the requirements related to the general security topic of the family. 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	Physical Protection
Audit and Accountability	Personnel Security
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

[13] 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.

2.2 DETERMINING COMPLIANCE TO CUI SECURITY REQUIREMENTS

Nonfederal organizations can determine compliance to the requirements for protecting the confidentiality of CUI by conducting security assessments (e.g., testing, evaluations, inspections, verification and validation, audits). They can also define the type of assessments required, the level of assessor independence desired (e.g., self-assessments, third-party, independent assessments), and the type of evidence needed to determine compliance to the CUI security requirements. The security assessment results (or findings) can provide such evidence including the extent to which the requirements have been satisfied. Such information is needed to effectively manage the risk associated with nonfederal information systems processing, storing, or transmitting CUI in external environments. Organizations can employ or leverage the security assessment procedures in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, to help generate the appropriate evidence needed to determine compliance to the CUI security requirements.

Security assessments can be effectively carried out at various stages in the system development life cycle[14] to increase the grounds for confidence, or assurance, that the security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have been satisfied and continue to be satisfied over time. Building an effective assurance case[15] to demonstrate that the CUI security requirements have been satisfied is a process that involves: (i) compiling evidence from a variety of sources and from a variety of activities conducted during the system development life cycle; and (ii) presenting this evidence in a manner that decision makers are able to use effectively in making risk-based decisions regarding the protection of CUI.

[14] There are typically five phases in a generic system development life cycle: (i) initiation; (ii) development/acquisition; (iii) implementation; (iv) operations and maintenance; and (v) disposition (disposal).

[15] An assurance case is a body of evidence organized into an argument demonstrating that some claim about an information system holds (i.e., is assured). An assurance case is needed when it is important to show that a system exhibits some complex property such as safety, security, or reliability.

CHAPTER THREE

THE REQUIREMENTS

SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

This chapter describes fourteen families of security requirements (including basic and derived requirements) for protecting the confidentiality of CUI in nonfederal information systems and organizations.[16] The security controls from NIST SP 800-53 associated with the basic and derived requirements are also listed for each family. Organizations can use SP 800-53 to obtain additional information related to the basic and derived security requirements (e.g., supplemental guidance related to each of the referenced security controls, the security capabilities achieved by satisfying the basic and derived requirements, and a catalog of optional controls that can be used to develop additional requirements if needed for specific situations). The footnotes associated with the basic and derived security requirements provide non-prescriptive, additional information to 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.

[16] While the primary purpose of this publication is to define requirements to protect the *confidentiality* of CUI, certain requirements may be more closely aligned with system and information *integrity* (e.g., derived security requirements associated with security controls CM-2, CM-3, CM-4, CM-5, CM-8, MA-3, MA-3(1), and MA-3(2)). There is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the information system level support both confidentiality and integrity. Thus, the integrity requirements (either basic or derived) have a significant, albeit indirect, effect on the ability of an organization to protect CUI.

3.1 ACCESS CONTROL

Basic Security Requirement: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Derived Security Requirements:

a. Control the flow of CUI in accordance with approved authorizations;[17]

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

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

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

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

f. Limit unsuccessful logon attempts;

g. Provide privacy and security notices consistent with applicable CUI rules;

h. Use session lock to prevent access/viewing of data after period of inactivity;

i. Terminate (automatically) a user session after a defined condition;

j. Monitor and control remote access sessions;

k. Employ cryptographic mechanisms to protect the confidentiality/integrity of remote access sessions;

l. Route remote access via managed access control points;[18]

m. Manage remote use of privileged access to security-relevant information;

n. Protect wireless access using authentication and encryption;

o. Control connection of mobile devices;

p. Encrypt CUI on mobile devices;

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

r. Limit use of organizational portable storage devices on external information systems; and

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

References: NIST Special Publication 800-53.

ACCESS CONTROL	AC-2; AC-3; AC-3(4); AC-4; AC-5; AC-6; AC-6(1); AC-6(2); AC-6(5); AC-6(9); AC-6(10); AC-7; AC-8; AC-11; AC-11(1); AC-12; AC-17(1); AC-17(2); AC-17(3); AC-17(4); AC-18; AC-18(1); AC-19; AC-19(5); AC-20; AC-20(1); AC-20(2); AC-22.

[17] Information flow control regulates where CUI is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.

[18] Limiting the number of access control points for remote accesses and controlling those access points reduces the attack surface for organizations and facilitates the use of managed interfaces (i.e., interfaces within an information system/network that provide boundary protection capability using automated mechanisms or devices).

3.2 AWARENESS AND TRAINING

Basic Security Requirement: Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, or procedures related to the security of organizational information systems; and ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.[19]

Derived Security Requirements: Provide security awareness training on recognizing and reporting potential indicators of insider threat.

References: NIST Special Publication 800-53.

AWARENESS AND TRAINING	AT-2; AT-2(2); AT-3.

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirement: 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; and 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:

a. Review and update audited events;

b. Alert in the event of an audit process failure;

c. 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;

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

e. Provide an information system capability that compares and synchronizes internal system clocks to generate time stamps for audit records;

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

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

References: NIST Special Publication 800-53.

AUDIT AND ACCOUNTABILITY	AU-2; AU-2(3); AU-3; AU-3(1); AU-5; AU-6; AU-6(1); AU-6(3); AU-7; AU-8; AU-8(1); AU-9; AU-9(4); AU-12.

3.4 CONFIGURATION MANAGEMENT

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

Derived Security Requirements:

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

[19] Training includes security awareness training on proper safeguarding/dissemination limitations for CUI and role-based training on how individuals and the organization respond to incidents involving CUI.

b. Employ the principle of least functionality by configuring the information system to provide only essential capabilities;[20]

c. Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services;[21] and

d. Apply deny by exception (blacklist) policy to prevent the use of unauthorized software.[22]

References: NIST Special Publication 800-53.

CONFIGURATION MANAGEMENT	CM-2; CM-4; CM-5; CM-6; CM-7; CM-7(1); CM-7(2); CM-7(4); CM-8.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirement: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Derived Security Requirements:

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

[20] Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements.

[21] Organizations can review functions and services provided by their information systems to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations can also consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Network/system scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems can help identify and prevent the use of prohibited functions, ports, protocols, and services.

[22] The process used to identify software programs that are not authorized to execute on an information system is commonly referred to as *blacklisting*, or a policy of allow all, deny by exception. Organizations can also require a stronger policy of deny all, allow by exception, commonly referred to as *whitelisting*. For either policy, organizations can determine what exceptions, if any, are acceptable (i.e., the deny by exception requirement does not necessarily imply that all restricted uses of nonessential functions have to be implemented by applying deny by exception methods, since some may not be practical to implement).

[23] 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. Mobile device technologies (e.g., smart phones) may also provide alternative token-based solutions for implementing multifactor authentication.

b. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts;[24]

c. Prevent reuse of identifiers for a defined period;

d. Disable identifiers after a defined period of inactivity;

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

f. Prohibit password reuse for a specified number of generations;

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

h. Store and transmit only encrypted representation of passwords; and

i. Obscure feedback of authentication information.

References: NIST Special Publication 800-53.

IDENTIFICATION AND AUTHENTICATION	IA-2; IA-2(1); IA-2(2); IA-2(3); IA-2(8); IA-2(9); IA-4; IA-5; IA-5(1); IA-6.

3.6 INCIDENT RESPONSE

Basic Security Requirement: Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate organizational officials and/or authorities.

Derived Security Requirements: None.

References: NIST Special Publication 800-53.

INCIDENT RESPONSE	IR-2; IR-3; IR-3(2); IR-4; IR-5; IR-6; IR-7.

3.7 MAINTENANCE

Basic Security Requirement: Perform periodic and timely maintenance on organizational information systems; and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.[25]

Derived Security Requirements:

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

b. Check media containing diagnostic and test programs for malicious code before the media are used in the information system;

c. Require strong authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete; and

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

[24] Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording or replaying previous authentication messages. Replay-resistant authentication techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

[25] This requirement includes both *local* and *nonlocal* (remote) system maintenance.

References: NIST Special Publication 800-53.

MAINTENANCE	MA-2; MA-3; MA-3(1); MA-3(2); MA-4; MA-5; MA-6.

3.8 MEDIA PROTECTION

Basic Security Requirement: Protect information system media containing CUI, both paper and digital; limit access to CUI on information system media to authorized users; and sanitize or destroy information system media containing CUI before disposal or release for reuse.

Derived Security Requirements:

a. Mark media with necessary CUI markings and distribution limitations;

b. Control/restrict access to media containing CUI during transport outside of controlled areas;

c. Prohibit the use of portable storage devices when such devices have no identifiable owner; and

d. Protect the confidentiality of backup CUI at storage locations.

References: NIST Special Publication 800-53.

MEDIA PROTECTION	MP-2; MP-3; MP-4; MP-5; MP-6; MP-7; MP-7(1); CP-9.

3.9 PHYSICAL PROTECTION

Basic Security Requirement: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals; and protect the physical plant and support infrastructure for those information systems.

Derived Security Requirements:

a. Escort visitors;

b. Monitor visitor activity; and

c. Maintain audit logs of physical access.

References: NIST Special Publication 800-53.

PHYSICAL PROTECTION	PE-2; PE-3; PE-5.

3.10 PERSONNEL SECURITY

Basic Security Requirement: Screen individuals prior to authorizing access to information systems containing CUI and ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Derived Security Requirements: None.

References: NIST Special Publication 800-53.

PERSONNEL SECURITY	PS-3; PS-4; PS-5.

3.11 RISK ASSESSMENT

Basic Security Requirement: 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:

a. Scan for vulnerabilities in the information system and applications and when new vulnerabilities affecting the system are identified; and

b. Remediate vulnerabilities in accordance with assessments of risk.

References: NIST Special Publication 800-53.

RISK ASSESSMENT	RA-3; RA-5.

3.12 SECURITY ASSESSMENT

Basic Security Requirement: Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Derived Security Requirements: None.

References: NIST Special Publication 800-53.

SECURITY ASSESSMENT	CA-2; CA-7.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirement: 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; and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Derived Security Requirements:

a. Separate user functionality from information system management functionality (e.g., privileged user functions);

b. Prevent unintended information transfer via shared system resources;

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

d. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);[26]

[26] This requirement: (i) applies to both inbound and outbound network communications traffic; and (ii) is typically implemented through managed interface devices for network access including gateways, routers, firewalls, guards, or combination thereof. These devices, when properly configured, allow connections only to approved sources. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

e. Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks;[27]

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

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

h. Establish and manage cryptographic keys for cryptography employed in the information system;

i. Employ FIPS-validated cryptography when used to protect confidentiality of CUI;

j. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device;

k. Manage the use of mobile code;[28]

l. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies and monitor/control use of VoIP;[29]

m. Protect the authenticity of communications sessions; and

n. Protect the confidentiality of CUI at rest.

References: NIST Special Publication 800-53.

SYSTEM AND COMMUNICATIONS PROTECTION	SC-2; SC-4; SC-7; SC-7(5); SC-7(7); SC-8; SC-8(1); SC-10; SC-12; SC-13; SC-15; SC-18; SC-19; SC-23; SC-28.

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirement: Identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response.

Derived Security Requirements:

a. Update malicious code protection mechanisms when new releases are available;

b. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed;

c. Monitor the information system to detect attacks and indicators of potential attacks; and

[27] This requirement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable *split tunneling* in those devices, and by preventing those configuration settings from being readily configurable by users. The requirement is implemented within the information system that the remote device is accessing by split tunneling detection (or of the configuration settings that allow split tunneling) in the remote device, and by prohibiting connections if remote devices are using split tunneling. Split tunneling can facilitate unauthorized external connections, making the system more vulnerable to attack and to exfiltration of CUI.

[28] Mobile code can be transferred between information systems and across networks and can be installed and executed on local systems (e.g., via email or web applications) without the explicit consent or knowledge of the organization or individual users. Examples of mobile code include JavaScript, ActiveX, and Flash animations. Mobile code can also represent a significant threat if such code is malicious and results in the unauthorized exfiltration of CUI. Organizations can manage mobile code usage by: (i) employing scanning tools to detect unauthorized mobile code; (ii) using digital signatures and other integrity-checking technologies to ensure the integrity of mobile code; and (iii) implementing either white or black listing policies though operating system configurations to restrict the use of mobile code.

[29] NIST SP 800-58 provides additional implementation guidance on the use of VoIP technologies.

d. Identify unauthorized use of the information system.

References: NIST Special Publication 800-53.

SYSTEM AND INFORMATION INTEGRITY	SI-2; SI-3; SI-4; SI-5.

APPENDIX A

REFERENCES

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

LEGISLATION, EXECUTIVE ORDERS, REGULATIONS, AND POLICIES

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Executive Order 13556, *Controlled Unclassified Information*, November 2010.

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 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
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*, August 2008.

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.

Controlled Unclassified Information [E.O. 13556]	Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and governmentwide policies, 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	Types of information that require safeguarding or dissemination controls pursuant to and consistent with law, regulation, and governmentwide policy, approved by the CUI Executive Agent, and listed in the CUI Registry.
CUI Executive Agent	The National Archives and Records Administration (NARA), which implements the governmentwide CUI Program and oversees federal agency actions to ensure that they comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
CUI Program	The rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, the CUI Registry, and additional issuances by the CUI Executive Agent.
CUI Registry	The online repository of information and policy regarding how authorized holders of CUI should handle such information. The CUI Registry: (i) identifies all of the categories and subcategories of information that require safeguarding and dissemination controls consistent with law, regulation, and governmentwide policies; (ii) provides descriptions for each category and subcategory; (iii) identifies the basis for safeguarding and dissemination controls; (iv) contains associated markings and applicable safeguarding, disseminating, and decontrolling procedures; and (v) specifies CUI that may be originated only by certain executive agencies and organizations. The CUI Executive Agent is the approval authority for all categories/subcategories of information identified as CUI in the CUI Registry and only those categories/subcategories listed are considered CUI.
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.
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.
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.
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. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
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.

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 smart phones, 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.

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.

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.

Sensitive Information [CNSSI 4009, Adapted]	Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act) that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
System	See *Information System*.
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.

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 Management Act
ISOO	Information Security Oversight Office
ITL	Information Technology Laboratory
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication