DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
SECURITY VARIANCE FORM FOR DATA ACCESS
NON-COMPLIANCE OF SECURITY REQUIREMENTS

The DOJRC requires this form to be completed and submitted in order to properly assess, document, and authorize exemption requests for non-compliance to the DOJRC Researcher Data Access User Agreement security requirements for the requestor's personally owned or organization provided laptop device. This form must be completed accurately and no fields left blank in order for the request to be processed. Submit the completed form to the DOJRC at DataRequests@doj.ca.gov and contact the DOJRC with any questions about this form and/or the procedure to request an exemption.

NOTE: If an exemption is approved and the California DOJ data is breached, corrupted, stolen, or lost due to the lack of security controls in place, the requestor and/or organization will be held liable and may be subject to civil and/or criminal prosecution.

Exemption request title:

Requesting organization/team:

Non-compliance to what security controls or requirements is being requested:

Exemption requested until:

1. Describe the exemption request. Provide detailed reasoning and justification for requesting the exemption.

2. Identify the security control or requirement that the requestor is unable to implement on their personally-owned or organization-issued information technology device/equipment. Why is the device/equipment not compliant, or cannot be made to be compliant? Provide a detailed explanation of the consequences if this request is not approved.

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
SECURITY VARIANCE FORM FOR DATA ACCESS
NON-COMPLIANCE OF SECURITY REQUIREMENTS

3. When will compliance occur? If compliance will take longer than one year, non-compliance will require annual exemption renewal.

4. Summarize the mitigation plan to minimize or compensate for the risk(s) associated with this exemption.

AUTHORIZATION

I (We) acknowledge all information provided herein is true and accurate to the best of my (our) knowledge. I (we) agree to accept any security risk to the DOJ data or system as a result of this security exception request. _____ **(Requestor initials here)**

Requestor Name: **Job Title:**

Requestor's Signature: **Date:**

I (We) acknowledge all information provided herein is true and accurate to the best of my (our) knowledge. I (we) agree to accept any security risk to the DOJ data or system as a result of this security exception request. _____ **(Requestor's Manager initials here)**

Manager Name: **Job Title:**

Manager Signature: **Date:**

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
SECURITY VARIANCE FORM FOR DATA ACCESS
NON-COMPLIANCE OF SECURITY REQUIREMENTS

Department of Justice Research Center Director:

Signature: **Date:**

Approved: Not Approved:

Department of Justice Information Security Officer:

Signature: **Date:**

Approved: Not Approved:

Comments:

Anticipated length of non-compliance:

NOTE: Exceptions will be valid (1) until compliance occurs or (2) for one year, whichever occurs first. If compliance will take longer than one year, a renewal is required. Renewals are not automatically approved and must be reviewed to ensure that assumptions have not changed and that compensating controls continue to mitigate risk to the DOJ.

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

Researcher Name:	Phone Number: Email Address:
Information Security Officer (ISO) ***or*** Information Technology (IT) Manager/Official's Name:	Phone Number: Email Address:
Organization Name:	Office/Branch: Address:
Organization Leader Name:	City, State, and Zip:

The following agreement has been established to address conditions when a researcher is authorized to establish a remote access connection to their organization's network to access DOJ data remotely using a personally-owned or organization-issued IT device/equipment. The researcher and their supervisor/manager and/or organization leadership are to acknowledge that they have read, understood, and agree to adhere to the requirements in this agreement.

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

Security precautions must be taken when accessing DOJ data remotely. The minimum security precautions include the following:

- Researchers who are accessing DOJ data located at their research organization must use Virtual Private Network encryption while remote. DOJ data must not be copied to a mobile device.
- Researchers must ensure that a host firewall is turned on at all times.
- DOJ data shall not be copied, duplicated, transferred, printed, or otherwise manipulated through the researcher's personal printing devices due to possible loss of control, and the unintentional storage of DOJ data.
- Researchers shall ensure that manufacturer-recommended security updates and configuration changes are applied regularly to the software on their personally-owned or organization-issued IT device/equipment that relate to security updates to fix vulnerabilities. Researchers shall ensure these updates are applied the software in the required timeframe specified by the vendor if it is used to remotely connect to their organization to access DOJ data.
- If an IT device/equipment from the researcher's organization is used to remotely connect to the researcher's organization to access DOJ data, the IT device/equipment must have all current security patches updated and have malware protections enabled.

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

The following is a checklist of the security controls or configurations that must be put in place if a researcher is accessing DOJ data from a personally-owned or organization-issued IT device/ equipment. Check each box to confirm compliance with the previously listed minimum security requirements.	
Ensure the firewall software included with the computer is turned on and set to block all incoming connections from other computers, outside sources on the Internet, and sources that have not been approved or permitted.	**I (we) confirm compliance:**
Disable non-essential services, such as file and print sharing.	**I (we) confirm compliance:**
Disable unnecessary networking features such as wireless network access features (e.g., IEEE 802.11a/b/ g/n, Bluetooth, and infrared).	**I (we) confirm compliance:**
Configure the personally-owned or organization-issued IT device/equipment so that they do not automatically attempt to join detected wireless networks.	**I (we) confirm compliance:**
Antivirus and antispyware software (software that detects and blocks malicious code).	**I (we) confirm compliance:** **Please identify what antivirus or antispyware is being used if it applies (e.g. Norton Anti-virus, McAfee, TotalAv, etc.):**
Remote access users shall review manufacturer documentation for each software program their personally-owned or organization-issued IT device/ equipment contains in these categories to determine each program's update capabilities and enable automatic updates where possible.	**I (we) confirm compliance:**
Web browser settings are securely configured, which requires, at a minimum, to keep the browser up to date, to block third party cookies, to block pop-ups, and to disable features that might cause vulnerabilities.	**I (we) confirm compliance:**

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

I (We) have read, understood, and acknowledge the DOJRC Researcher Data Access User Agreement. I (We) agree to comply with the agreement terms of the security controls that need to be put in place on my (our) personally-owned or organization-issued IT device/equipment before accessing DOJ data. If I am (we are) unable to comply with all the security requirements, a DOJRC Security Variance Form for Data Access Non-Compliance of Security Requirements form will be completed and submitted to DataRequests@doj.ca.gov to identify the security controls with which I am (we are) not in compliance and I (we) will identify a mitigation plan that will be used to minimize or compensate for the associated risk(s).

Employee Signature:	Date:
ISO/IT Manager/ Official Signature:	Date:
Organizational Leader Signature:	Date:

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER CONFIDENTIALITY AND NON-DISCLOSURE (CND) AGREEMENT

Company or Organization: _____

Researcher's Full Legal Name: _____

Researcher's Phone Number: _____

Researchers must complete all sections. The DOJRC will not process this CND Agreement with blank areas. Please attach supporting documentation if necessary.

The DOJ collects, stores, and disseminates confidential and sensitive information from the law enforcement community and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the State Administrative Manual, and in reference to associated DOJ information technology (IT) security policies. The DOJ prohibits unauthorized access, use, or disclosure of DOJ information or systems.

The following agreement has been established to address the confidentiality of DOJ data including but not limited to the California Law Enforcement Telecommunications System, California Justice Information Systems, law enforcement agency, and other DOJ data.

1. A researcher may access DOJ data when authorized by the DOJRC to fulfill research related work. Researchers may only disclose or release DOJ data to individuals that the DOJRC has authorized to receive it. Researchers may not access or use information from the DOJ network, information systems, applications, or from any databases accessible through the DOJ network, for any purpose not related to the research related work. Such use may be subject to administrative, civil, or criminal penalties.

_____ (initial here)

2. Researchers are prohibited from modifying, deleting, or destroying existing DOJ data, except as required in paragraph 4 after the conclusion of the research. _____ (initial here)

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC) RESEARCHER
CONFIDENTIALITY AND NON-DISCLOSURE (CND) AGREEMENT

3. Researchers must take precautions to protect DOJ data. Precautions include, but are not limited to, the following:

a. DOJ requires all researchers to utilize their associated organizations' IT hardware and equipment while working onsite or offsite and when accessing sensitive or confidential data including but not limited to personally identifiable information, Health Insurance Portability and Accountability Act, and DOJ data. _____ (initial here)
b. The researcher must ensure that their organizations desktop or laptop that is used to review or access DOJ data is locked at all times when left unattended. _____ (initial here)
c. Saving files on a researcher's desktop or laptop for file-sharing such as, peer-to-peer, Google drive, Dropbox, etc., or on USB drives, CD-ROMs or in a cloud environment is strictly prohibited. Storing DOJ data on the laptop is prohibited. _____ (initial here)
d. The researcher must immediately notify their organization's Information Security Officer, who must immediately contact the DOJ's Information Security Office, of any security incidents involving data or any incident regarding breaches of data. _____ (initial here)

4. Upon conclusion of the authorized research work, the researcher will provide the DOJRC with proof of destruction of all DOJ data. Destruction of DOJ data must comply with the National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1, Guidelines for Media Sanitation (December 2014) which is incorporated by reference. _____ (initial here)

I acknowledge that I have read and understood the information provided herein, and received a copy of the DOJRC Researcher CND Agreement. I understand that failure to comply with this agreement, and the applicable California laws and regulations governing the use and disclosure of the DOJ data, may result in administrative, civil, or criminal penalties under applicable California laws and regulations.

_____ (initial here)

NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

C O M P U T E R S E C U R I T Y

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

NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

December 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 in accordance with its statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 *et seq.*, Public Law 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 800-88 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-88 Revision 1, 64 pages (December 2014)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

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
Email: 800-88r1comments@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. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

Keywords

media sanitization; ensuring confidentiality; sanitization tools and methods; media types; mobile devices with storage; crypto erase; secure erase

Acknowledgements

The authors would like to thank Steven Skolochenko and Xing Li for their contributions to the original version of this publication. The authors would also like to thank Jim Foti for his exceptional editing skills and thorough review of this document – his work made this a much better document. Kudos to each of the individuals and organizations who provided comments on this revision. It is a more accurate and usable document due to their contributions.

The modern storage environment is rapidly evolving. Data may pass through multiple organizations, systems, and storage media in its lifetime. The pervasive nature of data propagation is only increasing as the Internet and data storage systems move towards a distributed cloud-based architecture. As a result, more parties than ever are responsible for effectively sanitizing media and the potential is substantial for sensitive data to be collected and retained on the media. This responsibility is not limited to those organizations that are the originators or final resting places of sensitive data, but also intermediaries who transiently store or process the information along the way. The efficient and effective management of information from inception through disposition is the responsibility of all those who have handled the data.

The application of sophisticated access controls and encryption help reduce the likelihood that an attacker can gain direct access to sensitive information. As a result, parties attempting to obtain sensitive information may seek to focus their efforts on alternative access means such as retrieving residual data on media that has left an organization without sufficient sanitization effort having been applied. Consequently, the application of effective sanitization techniques and tracking of storage media are critical aspects of ensuring that sensitive data is effectively protected by an organization against unauthorized disclosure. Protection of information is paramount. That information may be on paper, optical, electronic or magnetic media.

An organization may choose to dispose of media by charitable donation, internal or external transfer, or by recycling it in accordance with applicable laws and regulations if the media is obsolete or no longer usable. Even internal transfers require increased scrutiny, as legal and ethical obligations make it more important than ever to protect data such as Personally Identifiable Information (PII). No matter what the final intended destination of the media is, it is important that the organization ensure that no easily re-constructible residual representation of the data is stored on the media after it has left the control of the organization or is no longer going to be protected at the confidentiality categorization of the data stored on the media.

Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information. It does not, and cannot, specifically address all known types of media; however, the described sanitization decision process can be applied universally.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose and Scope

The information security concern regarding information disposal and media sanitization resides not in the media but in the recorded information. The issue of media disposal and sanitization is driven by the information placed intentionally or unintentionally on the media. Electronic media used on a system should be assumed to contain information commensurate with the security categorization of the system's confidentiality. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information. Categorization of an information technology (IT) system in accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*[1], is the critical first step in understanding and managing system information and media.

Based on the results of categorization, the system owner should refer to NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[2], which specifies that "the organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance. The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media."

This document will assist organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality.

The objective of this special publication is to assist with decision making when media require disposal, reuse, or will be leaving the effective control of an organization. Organizations should develop and use local policies and procedures in conjunction with this guide to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information.

The information in this guide is best applied in the context of current technology and applications. It also provides guidance for information disposition, sanitization, and control decisions to be made throughout the system life cycle. Forms of media exist that are not addressed by this guide, and media are yet to be developed and deployed that are not covered by this guide. In those cases, the intent of this guide outlined in the procedures section applies to all forms of media based on the evaluated security categorization of the system's confidentiality according to FIPS 199.

---

[1] Federal Information Processing Standards (FIPS) Publication 199 *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, 13 pp. http://csrc.nist.gov/publications/PubsFIPS.html#199.

[2] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (includes updates as of January 15, 2014), 460 pp. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Before any media are sanitized, system owners are strongly advised to consult with designated officials with privacy responsibilities (e.g., Privacy Officers), Freedom of Information Act (FOIA) officers, and the local records retention office. This consultation is to ensure compliance with record retention regulations and requirements in the Federal Records Act. In addition, organizational management should also be consulted to ensure that historical information is captured and maintained where required by business needs. This should be ongoing, as controls may have to be adjusted as the system and its environment changes.

1.2 Audience

Protecting the confidentiality of information should be a concern for everyone, from federal agencies and businesses to home users. Recognizing that interconnections and information exchange are critical in the delivery of government services, this guide can be used to assist in deciding what processes to use for sanitization or disposal.

1.3 Assumptions

The premise of this guide is that organizations are able to correctly identify the appropriate information categories, confidentiality impact levels, and location of the information. Ideally, this activity is accomplished in the earliest phase of the system life cycle.[3] This critical initial step is outside the scope of this document, but without this identification, the organization will, in all likelihood, lose control of some media containing sensitive information.

This guide does not claim to cover all possible media that an organization could use to store information, nor does it attempt to forecast the future media that may be developed during the effective life of this guide. Users are expected to make sanitization and disposal decisions based on the security categorization of the information contained on the media.

1.4 Relationship to Other NIST Documents

The following NIST documents, including FIPS and Special Publications, are directly related to this document:

- FIPS 199 and NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*[4], provide guidance for establishing the security categorization for a system's confidentiality. This categorization will impact the level of assurance an organization should require in making sanitization decisions.

[3] NIST SP 800-64 Revision 2, *Security Considerations in the Systems Development Life Cycle*, October 2008, 67 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-64.

[4] NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, 2 vols. http://csrc.nist.gov/publications/PubsSPs.html#800-60.

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*[5], sets a base of security requirements that requires organizations to have a media sanitization program.

- FIPS 140-2, *Security Requirements for Cryptographic Modules*[6], establishes a standard for cryptographic modules used by the U.S. Government.

- NIST SP 800-53 Revision 4 provides minimum recommended security controls, including sanitization, for Federal systems based on their overall system security categorization.

- NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*[7], provides guidance for assessing security controls, including sanitization, for federal systems based on their overall system security categorization.

- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*[8], provides guidance for selecting and using storage encryption technologies.

- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*[9], provides guidance for protecting the confidentiality of personally identifiable information in information systems.

1.5 Document Structure

The guide is divided into the following sections and appendices:

- **Section 1** (this section) explains the authority, purpose and scope, audience, assumptions of the document, relationships to other documents, and outlines its structure.

- **Section 2** presents an overview of the need for sanitization and the basic types of information, sanitization, and media.

---

[5] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006, 17 pp. http://csrc.nist.gov/publications/PubsFIPS.html#200.

[6] FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (includes change notices through December 3, 2002), 69 pp. http://csrc.nist.gov/publications/PubsFIPS.html#140-2.

[7] NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010, 399 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-53A.

[8] NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices,* November 2007, 40 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-111.

[9] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010, 59 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-122.

- **Section 3** provides an overview of relevant roles and responsibilities for the management of data throughout its lifecycle.
- **Section 4** provides the user with a process flow to assist with sanitization decision making.
- **Section 5** summarizes some general sanitization techniques.
- **Appendix A** specifies the minimum recommended sanitization techniques to Clear, Purge, or Destroy various media. This appendix is used with the decision flow chart provided in Section 4.
- **Appendix B** defines terms used in this guide.
- **Appendix C** lists tools and external resources that can assist with media sanitization.
- **Appendix D** contains considerations for selecting a storage device implementing Cryptographic Erase.
- **Appendix E** identifies a set of device-specific characteristics of interest that users should request from storage device vendors.
- **Appendix F** contains a bibliography of sources and correspondence that was essential in developing this guide.
- **Appendix G** provides a sample certificate of sanitization form for documenting an organization's sanitization activities.

2 Background

Information disposition and sanitization decisions occur throughout the information system life cycle. Critical factors affecting information disposition and media sanitization are decided at the start of a system's development. The initial system requirements should include hardware and software specifications as well as interconnections and data flow documents that will assist the system owner in identifying the types of media used in the system. Some storage devices support enhanced commands for sanitization, which may make sanitization easier, faster, and/or more effective. The decision may be even more fundamental, because effective sanitization procedures may not yet have been determined for emerging media types. Without an effective command or interface-based sanitization technique, the only option left may be to destroy the media. In that event, the media cannot be reused by other organizations that might otherwise have been able to benefit from receiving the repurposed storage device.

A determination should be made during the requirements phase about what other types of media will be used to create, capture, or transfer information used by the system. This analysis, balancing business needs and risk to confidentiality, will formalize the media that will be considered for the system to conform to FIPS 200.

Media sanitization and information disposition activity is usually most intense during the disposal phase of the system life cycle. However, throughout the life of an information system, many types of media, containing data, will be transferred outside the positive control of the organization. This activity may be for maintenance reasons, system upgrades, or during a configuration update.

2.1 Need for Proper Media Sanitization and Information Disposition

Media sanitization is one key element in assuring confidentiality. *Confidentiality* is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"[10] Additionally, "a loss of confidentiality is the unauthorized disclosure of information."[11]

In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. An often rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media, or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information. Media flows in and out of organizational control through recycle bins in paper form, out to vendors for equipment repairs, and hot swapped into other systems in response to hardware or software failures. This potential vulnerability can be mitigated through proper understanding of where information is located, what that information is, and how to protect it.

[10] "Definitions," Title 44 *U.S.Code*, Sec. 3542. 2006 ed. Supp. 5. Available: http://www.gpo.gov/; accessed 7/21/2014.

[11] FIPS 199, p.2.

2.2 Types of Media

There are two primary types of media in common use:

- **Hard Copy.** Hard copy media are physical representations of information, most often associated with paper printouts. However, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. The supplies associated with producing paper printouts are often the most uncontrolled. Hard copy materials containing sensitive data that leave an organization without effective sanitization expose a significant vulnerability to "dumpster divers" and overcurious employees, risking unwanted information disclosures.

- **Electronic (i.e., "soft copy").** Electronic media are devices containing bits and bytes such as hard drives, random access memory (RAM), read-only memory (ROM), disks, flash memory, memory devices, phones, mobile computing devices, networking devices, office equipment, and many other types listed in Appendix A.

In the future, organizations will be using media types not specifically addressed by this guide. The processes described in this document should guide media sanitization decision making regardless of the type of media in use. To effectively use this guide for all media types, organizations and individuals should focus on the information that could possibly have been recorded on the media, rather than on the media itself.

2.3 Trends in Data Storage Media

Historical efforts to sanitize magnetic media have benefitted from the wide use of a single common type of storage medium implemented relatively similarly across vendors and models. The storage capacity of magnetic media has increased at a relatively constant rate and vendors have modified the technology as necessary to achieve higher capacities. As the technology approaches the superparamagnetic limit, or the limit at which magnetic state can be changed with existing media and recording approaches, additional new approaches and technologies will be necessary in order for storage vendors to produce higher capacity devices.

Alternative technologies such as flash memory-based storage devices, or Solid State Drives (SSDs), have also become prevalent due to falling costs, higher performance, and shock resistance. SSDs have already begun changing the norm in storage technology, and—at least from a sanitization perspective—the change is revolutionary (as opposed to evolutionary). Degaussing, a fundamental way to sanitize magnetic media, no longer applies in most cases for flash memory-based devices. Evolutionary changes in magnetic media will also have potential impacts on sanitization. New storage technologies, and even variations of magnetic storage, that are dramatically different from legacy magnetic media will clearly require sanitization research and require a reinvestigation of sanitization procedures to ensure efficacy.

Both revolutionary and evolutionary changes make sanitization decisions more difficult, as the storage device may not clearly indicate what type of media is used for data storage. The burden falls on the user to accurately determine the media type and apply the associated sanitization procedure.

2.4 Trends in Sanitization

For storage devices containing *magnetic* media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data. One major drawback of relying solely upon the native Read and Write interface for performing the overwrite procedure is that areas not currently mapped to active Logical Block Addressing (LBA) addresses (e.g., defect areas and currently unallocated space) are not addressed. Dedicated sanitize commands support addressing these areas more effectively. The use of such commands results in a tradeoff because although they should more thoroughly address all areas of the media, using these commands also requires trust and assurance from the vendor that the commands have been implemented as expected.

Users who have become accustomed to relying upon overwrite techniques on magnetic media and who have continued to apply these techniques as media types evolved (such as to flash memory-based devices) may be exposing their data to increased risk of unintentional disclosure. Although the host interface (e.g. Advanced Technology Attachment (ATA) or Small Computer System Interface (SCSI)) may be the same (or very similar) across devices with varying underlying media types, it is critical that the sanitization techniques are carefully matched to the media.

Destructive techniques for some media types may become more difficult or impossible to apply in the future. Traditional techniques such as degaussing (for magnetic media) become more complicated as magnetic media evolves, because some emerging variations of magnetic recording technologies incorporate media with higher coercivity (magnetic force). As a result, existing degaussers may not have sufficient force to effectively degauss such media.

Applying destructive techniques to electronic storage media (e.g., flash memory) is also becoming more challenging, as the necessary particle size for commonly applied grinding techniques goes down proportionally to any increases in flash memory storage density. Flash memory chips already present challenges with occasional damage to grinders due to the hardness of the component materials, and this problem will get worse as grinders attempt to grind the chips into even smaller pieces.

Cryptographic Erase (CE), as described in Section 2.6, is an emerging sanitization technique that can be used in some situations when data is encrypted as it is stored on media. With CE, media sanitization is performed by sanitizing the cryptographic keys used to encrypt the data, as opposed to sanitizing the storage locations on media containing the encrypted data itself. CE techniques are typically capable of sanitizing media very quickly and could support partial sanitization, a technique where a subset of storage media is sanitization. Partial sanitization, sometimes referred to as selective sanitization, has potential applications in cloud computing and mobile devices. However, operational use of CE today presents some challenges. In some cases, it may be difficult to verify that CE has effectively sanitized media. This challenge, and possible approaches, is described in Section 4.7.3. If verification cannot be performed, organizations should use alternative sanitization methods that can be verified, or use CE in combination with a sanitization technique that can be verified.

A list of device-specific characteristics of interest for the application of sanitization techniques is

included in Appendix E. These characteristics can be used to drive the types of questions that media users should ask vendors, but ideally this information would be made readily available by vendors so that it can be easily retrieved by users to facilitate informed risk based sanitization decisions. For example, knowing the coercivity of the media can help a user decide whether or not the available degausser(s) can effectively degauss the media.

2.5 Types of Sanitization

Regarding sanitization, the principal concern is ensuring that data is not unintentionally released. Data is stored on media, which is connected to a system. This guidance focuses on the media sanitization component, which is simply data sanitization applied to a representation of the data as stored on a specific media type. Other potential concern areas exist as part of the system, such as for monitors, which may have sensitive data burned into the screen. Sensitive data stored in areas of the system other than storage media (such as on monitor screens) are not addressed by this document.

When media is repurposed or reaches end of life, the organization executes the system life cycle sanitization decision for the information on the media. For example, a mass-produced commercial software program contained on a DVD in an unopened package is unlikely to contain confidential data. Therefore, the decision may be made to simply dispose of the media without applying any sanitization technique. Alternatively, an organization is substantially more likely to decide that a hard drive from a system that processed PII needs sanitization prior to Disposal.

Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals.

The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on media type.

In organizations, information exists that is not associated with any categorized system. This information is often hard copy internal communications such as memoranda, white papers, and presentations. Sometimes this information may be considered sensitive. Examples may include internal disciplinary letters, financial or salary negotiations, or strategy meeting minutes. Organizations should label these media with their internal operating confidentiality levels and associate a type of sanitization described in this publication.

Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. The level of effort applied when attempting to retrieve data may range widely. For example, a party may attempt simple keyboard attacks without the use of specialized tools, skills, or knowledge of the media characteristics. On the other end of the spectrum, a party may have extensive capabilities and be able to apply state of the art laboratory techniques.

Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

A more detailed summary of sanitization techniques is provided in Section 5. Sanitization requirements for specific media/device types are provided in Appendix A.

It is suggested that the user of this guide categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, the organization can choose the appropriate type(s) of sanitization. The selected type(s) should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process.

2.6 Use of Cryptography and Cryptographic Erase

Many storage manufacturers have released storage devices with integrated encryption and access control capabilities, also known as Self-Encrypting Drives (SEDs). SEDs feature always-on encryption that substantially reduces the likelihood that unencrypted data is inadvertently retained on the device. The end user cannot turn off the encryption capabilitieswhich ensures that all data in the designated areas are encrypted. A significant additional benefit of SEDs is the opportunity to tightly couple the controller and storage media so that the device can directly address the location where any cryptographic keys are stored, whereas solutions that depend only on the abstracted user access interface through software may not be able to directly address those areas.

SEDs typically encrypt all of the user-addressable area, with the potential exception of certain clearly identified areas, such as those dedicated to the storage of pre-boot applications and associated data.

Cryptographic Erase (CE) leverages the encryption of target data by enabling sanitization of the target data’s encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read-access.

Without the encryption key used to encrypt the target data, the data is unrecoverable. The level of effort needed to decrypt this information without the encryption key then is the lesser of the

strength of the cryptographic key or the strength of the cryptographic algorithm and mode of operation used to encrypt the data.

If strong cryptography is used, sanitization of the target data is reduced to sanitization of the encryption key(s) used to encrypt the target data. Thus, with CE, sanitization may be performed with high assurance much faster than with other sanitization techniques. The encryption itself acts to sanitize the data, subject to constraints identified in this guidelines document. Federal agencies must use FIPS 140 validated encryption modules[12] in order to have assurance that the conditions stated above have been verified for the SED.

Typically, CE can be executed in a fraction of a second. This is especially important as storage devices get larger resulting in other sanitization methods take more time. CE can also be used as a supplement or addition to other sanitization approaches.

2.6.1 When Not To Use CE To Purge Media

- Do not use CE to purge media if the encryption was enabled after sensitive data was stored on the device without having been sanitized first.
- Do not use CE if it is unknown whether sensitive data was stored on the device without being sanitized prior to encryption.

2.6.2 When to Consider Using CE

- Consider using CE when all data intended for CE is encrypted prior to storage on the media (including the data, as well as virtualized copies).
- Consider using CE when we know the location(s) on the media where the encryption key is stored (be it the target data's encryption key or an associated wrapping key) and can sanitize those areas using the appropriate media-specific sanitization technique, ensuring the actual location on media where the key is stored is addressed.
- Consider using CE when we can know that all copies of the encryption keys used to encrypt the target data are sanitized
- Consider using CE when the target data's encryption keys are, themselves, encrypted with one or more wrapping keys and we are confident that we can sanitize the corresponding wrapping keys.
- Consider using CE when we are confident of the ability of the user to clearly identifyand use the commands provided by the device to perform the CE operation.

[12] NIST maintains lists of validated cryptographic modules (http://csrc.nist.gov/groups/STM/cmvp/validation.html) and cryptographic algorithms (http://csrc.nist.gov/groups/STM/cavp/validation.html).

2.6.3 Additional CE Considerations

If the encryption key exists outside of the storage device (typically due to backup or escrow), there is a possibility that the key could be used in the future to recover data stored on the encrypted media.

CE should only be used as a sanitization method when the organization has confidence that the encryption keys used to encrypt the Target Data have been appropriately protected. Such assurances can be difficult to obtain with software cryptographic modules, such as those used with software-based full disk encryption solutions, as these products typically store cryptographic keys in the file system or other locations on media which are accessible to software. While there may be situations where use of CE with software cryptographic modules is both appropriate and advantageous, such as performing a quick remote wipe on a lost mobile device, unless the organization has confidence in both the protection of the encryption keys, and the destruction of all copies of those keys in the sanitization process, CE should be used in combination with another appropriate sanitization method.

Sanitization using CE should not be trusted on devices that have been backed-up or escrowed the key(s) unless the organization has a high level of confidence about how and where the keys were stored and managed outside the device. Such back-up or escrowed copies of data, credentials, or keys should be the subject of a separate device sanitization policy. That policy should address backups or escrowed copies within the scope of the devices on which they are actually stored.

A list of applicable considerations, and a sample for how vendors could report the mechanisms implemented, is included in Appendix E. Users seeking to implement CE should seek reasonable assurance from the vendor (such as the vendor's report as described in Appendix E) that the considerations identified here have been addressed and only use FIPS 140 validated cryptographic modules.

2.7 Factors Influencing Sanitization and Disposal Decisions

Several factors should be considered along with the security categorization of the system confidentiality when making sanitization decisions. The cost versus benefit tradeoff of a sanitization process should be understood prior to a final decision. For instance, it may not be cost-effective to degauss inexpensive media such as diskettes. Even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and verification, etc.) to destroy media rather than use one of the other options. Organizations retain the ability increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk.

Organizations should consider environmental factors including (but not limited to):

- What types (e.g., optical non-rewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the confidentiality requirement for the data stored on the media?

- Will the media be processed in a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media? [13]
- What is the availability of sanitization equipment and tools?
- What is the level of training of personnel with sanitization equipment/tools?
- How long will sanitization take?
- What is the cost of sanitization when considering tools, training, verification, and re-entering media into the supply stream?

2.8 Sanitization Scope

For most sanitization operations, the target of the operation is all data stored on the media by the user. However, in some cases, there may be a desire or need to sanitize a subset of the media. Partial sanitization comes with some risk, as it may be difficult to verify that sensitive data stored on a portion of the media did not spill over into other areas of the media (e.g., remapped bad blocks). In addition, the dedicated interfaces provided by storage device vendors for sanitization typically operate at the device level, and are not able to be applied to a subset of the media. As a result, partial sanitization usually depends on the typical read and write commands available to the user, which may not be able to bypass any interface abstraction that may be present in order to directly address the media area of concern.

On some storage devices featuring integrated encryption capabilities, CE provides a unique mechanism for supporting some forms of partial sanitization. Some of these devices support the ability to encrypt portions of the data with different encryption keys (e.g., encrypting different partitions with different encryption keys). When the interface supports sanitizing only a subset of the encryption keys, partial sanitization via CE is possible. As with any other sanitization technique applied to media, the level of assurance depends both upon vendor implementation and on the level of assurance that data was stored only in the areas that are able to be reliably sanitized. Data may be stored outside these regions either because the user or software on the system moved data outside of the designated area on the media, or because the storage device stored data to the media in a manner not fully understood by the user.

Due to the difficulty in reliably ensuring that partial sanitization effectively addresses all sensitive data, sanitization of the whole device is preferred to partial sanitization whenever possible. Organizations should understand the potential risks to this approach and make appropriate decisions on this technique balancing the factors described earlier in this sectionas

[13] NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003, 67 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-36.

well as their business missions and specific use cases. For example, a drive in a datacenter may contain customer data from multiple customers. When one customer discontinues service and another begins storing data on the same media, the organization may choose to apply partial sanitization in order to retain the data of other customers that is also stored on the same storage device on other areas of the media. The organization may choose to apply partial sanitization because the drive remains in the physical possession of the organization, access by the customer is limited to the interface commands, and the organization has trust in the partial sanitization mechanism available for that specific piece of media. In cases where the alternative to partial sanitization is not performing sanitization at all, partial sanitization provides benefits that should be considered.

3 Roles and Responsibilities

3.1 Program Managers/Agency Heads

"Ultimately, responsibility for the success of an organization lies with its senior managers."[14] By establishing an effective information security governance structure, they establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the program and for ensuring program success. Senior management is responsible for ensuring that the resources are allocated to correctly identify types and locations of information and to ensure that resources are allocated to properly sanitize the information.

The other responsibilities in the remainder of this section are for illustrative purposes and the intent is to ensure that organizations think through the different responsibilities for sanitizing media and assign those responsibilities appropriately.

3.2 Chief Information Officer (CIO)

The CIO[15] is charged with promulgating information security policy. A component of this policy is information disposition and media sanitization. The CIO, as the information custodian, is responsible for ensuring that organizational or local sanitization requirements follow the guidelines of this document.

3.3 Information System Owner

The information system owner[16] should ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the impact of disclosure of such information on the organization.

3.4 Information Owner/Steward

The information owner should ensure that appropriate supervision of onsite media maintenance by service providers occurs, when necessary. The information owner is also responsible for ensuring that they fully understand the sensitivity of the information under their control and that the users of the information are aware of its confidentiality and the basic requirements for media sanitization.

---

[14]NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, 16. http://csrc.nist.gov/publications/PubsSPs.html#800-18.

[15]Per the Information Technology Management Reform Act of 1996 ("Clinger-Cohen Act"; P.L. 104-106 (Division E) 10 Feb. 1996), when an agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

[16]The role of the information system owner can be interpreted in a variety of ways depending on the particular agency and the system development life-cycle phase of the information system. Some agencies may refer to the information system owners as "program managers" or "business/asset/mission owners".

3.5 Senior Agency Information Security Officer (SAISO)

The SAISO is responsible for ensuring that the requirements of the information security policy with regard to information disposition and media sanitization are implemented and exercised in a timely and appropriate manner throughout the organization. The SAISO also requires access to the technical basis/personnel to understand and properly implement the sanitization procedures.

3.6 System Security Manager/Officer

Often assisting system management officials in this effort is a system security manager/officer responsible for day-today security implementation/administration duties. Although not normally part of the computer security program management office, this person is responsible for coordinating the security efforts of a particular system(s). This role is sometimes referred to as the Computer System Security Officer or the Information System Security Officer.

3.7 Property Management Officer

The property management officer is responsible for ensuring that sanitized media and devices that are redistributed within the organization, donated to external entities or destroyed are properly accounted for.

3.8 Records Management Officer

The records management officer is responsible for advising the system and/or data owner or custodian of retention requirements that must be met so the sanitization of media will not destroy records that should be preserved.

3.9 Privacy Officer

The privacy officer is responsible for providing advice regarding the privacy issues surrounding the disposition of privacy information and the media upon which it is recorded.

3.10 Users

Users have the responsibility for knowing and understanding the confidentiality of the information they are using to accomplish their assigned work and ensure proper handling of information.

4 Information Sanitization and Disposition Decision Making

An organization may maintain storage devices with differing levels of confidentiality, and it is important to understand what types of data may be stored on the device in order to apply the techniques that best balance efficiency and efficacy to maintain the confidentiality of the data. Data confidentiality level should be identified using procedures described in FIPS 199. Additional information is available on mapping information types to security categories in SP 800-60 Revision 1.

While most devices support some form of Clear, not all devices have a reliable Purge mechanism. For moderate confidentiality data, the media owner may choose to accept the risk of applying Clear techniques to the media, acknowledging that some data may be able to be retrieved by someone with the time, knowledge, and skills to do so.

Purge (and Clear, where applicable) may be more appropriate than Destroy when factoring in environmental concerns, the desire to reuse the media (either within the organization or by selling or donating the media), the cost of a media or media device, or difficulties in physically Destroying some types of media.

The risk decision should include the potential consequence of disclosure of information retrievable from the media, the cost of information retrieval and its efficacy, and the cost of sanitization and its efficacy. Additionally, the length of time the data will remain sensitive should also be considered. These values may vary between different environments.

Organizations can use Figure 4-1 with the descriptions in this section to assist them in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. The decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.

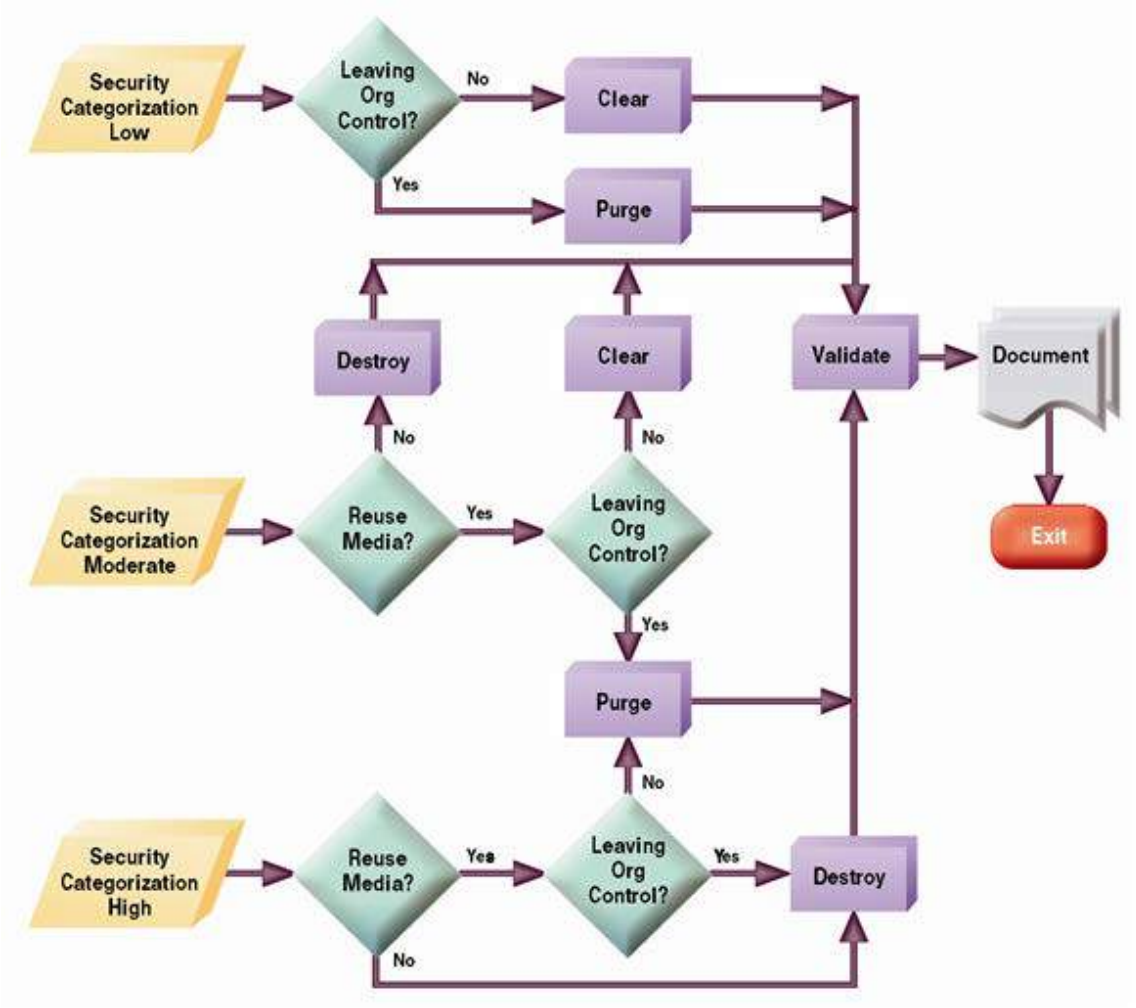

Figure 4-1: Sanitization and Disposition Decision Flow

4.1 Information Decisions in the System Life Cycle

The need for, and methods to conduct, media sanitization should be identified and developed before arriving at the Disposal phase in the system life cycle. At the start of system development, when the initial system security plan is developed[17], media sanitization controls are developed, documented, and deployed. One of the key decisions that will affect the ability to conduct sanitization is choosing what media are going to be used within the system. Although this is

[17] NIST SP 800-18 Revision 1, p.19.

mostly a business decision, system owners must understand early on that this decision affects the types of resources needed for sanitization throughout the rest of the system life cycle.

An organization may ask a product vendor for assistance in identifying storage media that may contain sensitive data. This information is typically documented in a 'statement of volatility'. The statement may be used to support decisions about which equipment to purchase, based on the ease or difficulty of sanitization. While volatility statements are useful, caution should be applied in comparing statements across vendors because vendors may state volatility details differently.

Organizations should take care in identifying media for sanitization. Many items used will contain multiple forms of media that may require different methods of sanitization. For example, a desktop computer may contain a hard drive, motherboard, RAM, and ROM, and mobile devices contain on-board volatile memory as well as nonvolatile removable memory.

The increasing availability of rapidly applicable techniques, such as Cryptographic Erase, provides opportunities for organizations to reduce the risk of inadvertent disclosure by combining sanitization technologies and techniques. For example, an organization could choose to apply Cryptographic Erase at a user's desktop before removing the media to send it to be 'formally' sanitized at the sanitization facility, in order to reduce risk and exposure.

4.2 Determination of Security Categorization

Early in the system life cycle, a system is categorized using the guidance found in FIPS 199, NIST SP 800-60 Rev. 1, or CNSSI 1253[18], including the security categorization for the system's confidentiality. This security categorization is revisited at least every three years (or when significant change occurs within the system) and revalidated throughout the system's life, and any necessary changes to the confidentiality category can be made. Once the security categorization is completed, the system owner can then design a sanitization process that will ensure adequate protection of the system's information.

Much information is not associated with a specific system but is associated with internal business communications, usually on paper. Organizations should label these media with their internal operating confidentiality levels and associate a type of sanitization described in this publication.

4.3 Reuse of Media

A key decision on sanitization is whether the media are planned for reuse or recycle. Some forms of media are often reused to conserve an organization's resources.

If media are not intended for reuse either within or outside an organization due to damage or other reason, the simplest and most cost-effective method of control may be Destroy.

[18] Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

4.4 Control of Media

A factor influencing an organizational sanitization decision is who has control and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organization. The following are examples of media control:

Under Organization Control:

- Media being turned over for maintenance are still considered under organization control if contractual agreements are in place with the organization and the maintenance provider specifically provides for the confidentiality of the information.
- Maintenance being performed on an organization's site, under the organization's supervision, by a maintenance provider is also considered under the control of the organization.

Not Under Organization Control (External Control):

- Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization are considered to be out of organizational control.

4.5 Data Protection Level

Even within an organization, varying data protection policies may be established. For instance, a company may have an engineering department and a sales department. The sales personnel may not have a need for access to the detailed proprietary technical data such as source code and schematics, and the engineers may not have a need to access the PII of the company's customers. Both might be within the same confidentiality categorization, but contextually different and with different internal and external rules regarding necessary controls. As such, data protection level is a complementary consideration to organizational control. When identifying whether sanitization is necessary, both the organizational control and data protection level should be considered.

4.6 Sanitization and Disposal Decision

Once an organization completes an assessment of its system confidentiality, determines the need for information sanitization, determines appropriate time frames for sanitization, and determines the types of media used and the media disposition, an effective, risk-based decision can be made on the appropriate and needed level of sanitization. Again, environmental factors and media type might cause the level of sanitization to change. For example, purging paper copies generally does not make sense, so destroying them would be an acceptable alternative.

Upon completion of sanitization decision making, the organization should record the decision and ensure that a process and proper resources are in place to support these decisions. This process is often the most difficult piece of the media sanitization process because it includes not only the act of sanitization but also the verification: capturing decisions and actions, identifying resources, and having critical interfaces with key officials.

4.7 Verify Methods

Verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. Two types of verification should be considered. The first is verification every time sanitization is applied (where applicable, as most Destroy techniques do not support practical verification for each sanitized piece of media). The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action. If sampling is done after full verification in cases of low risk tolerance then a different verification tool than the one used in the original verification should be used.

4.7.1 Verification of Equipment

Verification of the sanitization process is not the only assurance required by the organization. If the organization is using sanitization tools (e.g., a degausser or a dedicated workstation), then equipment calibration, as well as equipment testing, and scheduled maintenance, is also needed.

4.7.2 Verification of Personnel Competencies

Another key element is the potential training needs and current expertise of personnel conducting the sanitization. Organizations should ensure that equipment operators are competent to perform sanitization functions.

4.7.3 Verification of Sanitization Results

The goal of sanitization verification is to ensure that the target data was effectively sanitized. When supported by the device interface (such as an ATA or SCSI storage device or solid state drive), the highest level of assurance of effective sanitization (outside of a laboratory) is typically achieved by a full reading of all accessible areas to verify that the expected sanitized value is in all addressable locations. A full verification should be performed if time and external factors permit. This manner of verification typically only applies where the device is in an operational state following sanitization so that data can be read and written through the native interface.

If an organization chooses representative sampling then there are three main goals applied to electronic media sanitization verification:

1. Select pseudorandom locations on the media each time the analysis tool is applied. This reduces the likelihood that a sanitization tool that only sanitizes a subset of the media will result in verification success in a situation where sensitive data still remains.

2. Select locations across the addressable space (user addressable and reserved areas). For instance, conceptually break the media up into equally sized subsections. Select a large enough number of subsections so that the media is well-covered. The number of practical subsections depends on the device and addressing scheme. The suggested minimum number of subsections for a storage device leveraging LBA

addressing is one thousand. Select at least two non-overlapping pseudorandom locations from within each subsection. For example, if one thousand conceptual subsections are chosen, at least two pseudorandom locations in the first thousandth of the media addressing space would be read and verified, at least two pseudorandom locations in the second thousandth of the media addressing space would be read and verified, and so on.

   a. In addition to the locations already identified, include the first and last addressable location on the storage device.

3. Each consecutive sample location (except the ones for the first and last addressable location) should cover at least 5 % of the subsection and not overlap the other sample in the subsection. Given two non-overlapping samples, the resulting verification should cover at least 10 % of the media once all subsections have had two samples taken.

Cryptographic Erase has different verification considerations than procedures such as rewriting or block erasing, because the contents of the physical media following Cryptographic Erase may not be known and therefore cannot be compared to a given value. When Cryptographic Erase is leveraged, there are multiple options for verification, and each uses a quick review of a subset of the media. Each involves a selection of pseudorandom locations to be sampled from across the media.

The first option is to read the pseudorandom locations prior to Cryptographic Erase, and then again following Cryptographic Erase to compare the results. This is likely the most effective verification technique. Another option is to search for strings across the media or looking for files that are in known locations, such as operating system files likely to be stored in a specific area.

The number of locations and size of each sample should take into consideration the risks in transferring the Target Data to the storage media of the machine hosting the sanitization application. As a result, the proportion of the media covered by verification for the Cryptographic Erase technique may be relatively small (or at least lower than the above guidance of 10 % for verification of non-cryptographic sanitization techniques), but should still be applied across a wide range of the addressable area.

However, these techniques may not always be available because the individual performing the sanitization may not have the authentication token needed to access and read the data stored on the drive. If an organization cannot verify that CE effectively sanitized storage media, organizations should employ an alternative sanitization method that can be verified, either in combination with CE or in place of CE.

As part of the sanitization process, in addition to the verification performed on each piece of media following the sanitization operation, a subset of media items should be selected at random for secondary verification using a different verification tool. The secondary verification tool should be from a separate developer. For the secondary verification, a full verification should be performed. At least 20 % of sanitized media (by number of media

items sanitized) should be verified. The secondary verification provides assurance that the primary operation is working as expected.

4.8 Documentation

Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. A certification of media disposition may be a piece of paper or an electronic record of the action taken. For example, most modern hard drives include bar codes on the label for values such as model and serial numbers. The person performing the sanitization might simply enter the details into a tracking application and scan each bar code as the media is sanitized. Automatic documentation can be important as some systems make physical access to the media very difficult.

The decision regarding whether to complete a certificate of media disposition and how much data to record depends on the confidentiality level of the data on the media. For a large number of devices with data of very low confidentiality, an organization may choose not to complete the certificate.

When fully completed, the certificate should record at least the following details:

- Manufacturer
- Model
- Serial Number
- Organizationally Assigned Media or Property Number (if applicable)
- Media Type (i.e., magnetic, flash memory, hybrid, etc.)
- Media Source (i.e., user or computer the media came from)
- Pre-Sanitization Confidentiality Categorization (optional)
- Sanitization Description (i.e., Clear, Purge, Destroy)
- Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
- Tool Used (including version)
- Verification Method (i.e., full, quick sampling, etc.)
- Post-Sanitization Confidentiality Categorization (optional)
- Post-Sanitization Destination (if known)
- For Both Sanitization and Verification:
    - Name of Person

- Position/Title of Person
- Date
- Location
- Phone or Other Contact Information
- Signature

Optionally, an organization may choose to record the following (if known):

- Data Backup (i.e., if data was backed up, and if so, where)

A sample certificate is included in Appendix G.

If the storage device has been successfully verified and the sanitization results in a lower confidentiality level of the storage device, all markings on the device indicating the previous confidentiality level should be removed. A new marking indicating the updated confidentiality level should be applied, unless the device is leaving the organization and is stored in a location where access is carefully controlled until the device leaves the organization to prevent reintroduction of sensitive data.

The value of a certification of media disposition depends on the organization's handling of storage media over the media's lifecycle. If records are maintained when the media is introduced to the environment, when the media leaves the place it was last used, and when it reaches the sanitization destination, the organization can most effectively identify how well media sanitization is being applied across the enterprise. If there is a breakdown in tracking at locations other than the sanitization destination, the sanitization records only show that specific media was sanitized and not whether the organization is effectively sanitizing all media that has been introduced into the operating environment.

5 Summary of Sanitization Methods

Several different methods can be used to sanitize media. Four of the most common are presented in this section. Users of this guide should categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, using information in Table 5-1, decide on the appropriate method for sanitization. The selected method should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risks to an unauthorized disclosure of information.

Table 5-1: Sanitization Methods

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user-addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing

Method	Description
	renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

Appendix A Minimum Sanitization Recommendations

Once a decision is made based on factors such as those described in Section 4, and after applying relevant organizational environmental factors, then the tables in this Appendix can be used to determine recommended sanitization of specific media. That recommendation should reflect the FIPS 199 security categorization of the system confidentiality to reduce the impact of harm of unauthorized disclosure of information from the media.

Although use of the tables in this Appendix is recommended here, other methods exist to satisfy the intent of Clear, Purge, and Destroy. Methods not specified in this table may be suitable as long as they are verified and found satisfactory by the organization. Not all types of available media are specified in this table. If your media are not included in this guide, organizations are urged to identify and use processes that will fulfill the intent to Clear, Purge, or Destroy their media.

When an organization or agency has a sanitization technology, method and/or tool that they trust and have tested, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website[19]. The FASP effort was initiated as a result of the success of the Federal Chief Information Officer (CIO) Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection (CIP) and security.

The proper initial configuration of each type of device helps ensure that the sanitization operation is as effective as possible. While called out for some specific items below, users are encouraged to check manufacturer recommendations and guides such as the DISA Security Technical Implementation Guides (STIGs)[20] for additional information about recommended settings for any other items in this list as well.

If a mobile device has nonvolatile removable memory, it may contain additional information that may or may not be addressed by the sanitization process identified in Table A-3. Contact the manufacturer and/or cellular provider to determine what types of data are stored on the removable memory and identify whether any additional sanitization is required for the removable memory. Additional details about such removable memory and associated data recovery capabilities are available in NIST SP 800-101 Revision 1[21]. If a mobile device does not have sufficient built-in sanitization appropriate for the sensitivity or impact level of the data it contains, then rather than destroy the device (to protect the information) consider contacting businesses providing sanitization services to determine if their services meet your needs.

Many internal storage devices (as opposed to removable media, such as an SD card) as well as storage subsystems that incorporate installed media, support dedicated sanitize commands. The

[19] http://csrc.nist.gov/groups/SMA/fasp/

[20] http://iase.disa.mil/stigs/

[21] NIST SP 800-101 Revision 1, *Guidelines on Mobile Device Forensics*, May 2014, 87 pp. http://dx.doi.org/10.6028/NIST.SP.800-101r1.

availability of these commands is impacted in some cases by system (i.e., BIOS/UEFI—Basic Input-Output System/Unified Extensible Firmware Interface) characteristics, such as how and when freeze lock commands are issued to a device. The use of a dedicated computer or equipment to perform sanitization that facilitates leveraging these commands (such as a PC or workstation, with an external drive bay that facilitates safely connecting a drive after the system has been powered on) can help address this issue. The behavior and methods to bypass freeze lock or other limitations on command availability vary between computers, so refer to the computer manufacturer for details about the behavior of specific models. Alternative approaches exist for addressing the issue, and will vary depending on the hardware, software, and firmware of the computer. University of California San Diego (UCSD)'s Center for Magnetic Recording Research (CMRR) has also developed some tools and documentation about work-arounds for this issue (see Appendix C for details).

Some sanitization procedures feature additional optional methods. The choice regarding whether to apply the optional components depends on the level of confidentiality of the data and assurance of correct implementation of the non-optional portion of the sanitization procedure. For example, an organization might decide that for PII, for example, that any method applied with an available optional component should execute that optional component. The choice may also be based on the time factor, as some procedures, including the optional method, can be executed in a total of a matter of minutes. In that case, the organization might decide to include the optional component even if the data is not in a higher confidentiality category.

Table A-1: Hard Copy Storage Sanitization

Hard Copy Storage	
Paper and microforms	
Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.
Notes:	When material is burned, residue must be reduced to white ash.

Table A-2: Networking Device Sanitization

Networking Devices	
Routers and Switches (home, home office, enterprise)	
Clear:	Perform a full manufacturer's reset to reset the router or switch back to its factory default settings.

Purge:	See Destroy. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper Sanitization procedure. Network Devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.

Table A-3: Mobile Device Sanitization

Mobile Devices **(If a device has removable storage – first check for encryption and unencrypt if so – then remove the removable storage prior to sanitization)**	
Apple iPhone and iPad (current generation and future iPhones and iPads)	
Clear:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes as Cryptographic Erase is supported. This assumes that encryption is on and that all data has been encrypted.) Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes with Cryptographic Erase being supported. This assumes that encryption is on and that all data has been encrypted.)
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing the device, ensure that the data is backed up to a safe place. Current iPhones have hardware encryption – turned on by default.
Blackberry	**(back up data on device before sanitization)**
Clear:	BB OS 7.x/6.x - Select Options > Security Options > Security Wipe , making sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x) BB OS 10.x (Decrypt media card before continuing) Select Settings, Security and Privacy, Security Wipe . Type "blackberry" in the text field, then click on "Delete Data". The sanitization operation may take as long as several hours depending on the media size. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	BB OS 7.x/6.x - Select Options > Security > Security Wipe, then make sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x). For BB OS 10.x Select Settings> Security and Privacy>Security Wipe. Type "blackberry" in the text field, then click on "Delete Data". The

	sanitization operation may take as long as several hours depending on the media size.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Centralized management (BES) allows for device encryption. Refer to the manufacturer for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. If the device contains removable storage media, ensure that the media is sanitized using appropriate media-dependent procedures.
Devices running the Google Android OS (connect to power before starting encryption)	
Clear:	Perform a factory reset through the device's settings menu. For example, on Samsung Galaxy S5 running Android 4.4.2, select settings, then, under User and Backup, select Backup and reset, then select Factory data reset. For other versions of Android and other mobile phone devices, refer to the user manual. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Android devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). Some versions of Android support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. When in doubt, check device manual or call tech support. For both Clear and Purge, refer to the manufacturer for additional information on the proper sanitization procedure.
Windows Phone OS 7.1/8/8.x (Centralized management may be needed for encryption)	
Clear:	Select the Settings option (little gear symbol) from the live tile or from the app list. On the "Settings" page, scroll to the bottom of the page and select the "About" button. In the about page, there will be a **reset your phone** button at the bottom of the page. Click on this button to continue. Choose Yes when you see the warning messages. Please note that after the process is completed, all your personal content will disappear. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Windows Phone devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset

	option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). In some environments, Windows Phone devices may support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing your device, ensure that you back up your data to a safe location. Refer to the manufacturer for proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible.
All other mobile devices *This includes cell phones, smart phones, PDAs, tablets, and other devices not covered in the preceding mobile categories.*	
Clear:	Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	See Destroy. Many mobile devices only offer capabilities to Clear (and not Purge) the data contents. A mobile device may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to in order to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device. For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure.

Table A-4: Equipment Sanitization

Equipment	
Office Equipment *This includes copy, print, fax, and multifunction machines*	

Clear:	Perform a full manufacturer's reset to reset the office equipment to its factory default settings.
Purge:	See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For both Clear and (if applicable) Purge, manually navigate to multiple areas of the device (such as stored fax numbers, network configuration information, etc.) to verify that no personal information has been retained on the device. For both Clearing and (if applicable) Purge, the ink, toner, and associated supplies (drum, fuser, etc.) should be removed and destroyed or disposed of in accordance with applicable law, environmental, and health considerations. Some of these supplies may retain impressions of data printed by the machine and therefore could pose a risk of data exposure, and should be handled accordingly. If the device is functional, one way to reduce the associated risk is to print a blank page, then an all-black page, then another blank page. For devices with dedicated color components (such as cyan, magenta, and yellow toners and related supplies), one page of each color should also be printed between blank pages. The resulting sheets should be handled at the confidentiality of the Office Equipment (prior to sanitization). Note that these procedures do not apply to supplies such as ink/toner on a one-time use roll, as they are typically not used again and therefore will not be addressed by sending additional pages through the equipment. They will, however, still need to be removed and destroyed. Office Equipment supplies may also pose health risks, and should be handled using appropriate procedures to minimize exposure to the print components and toner. For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper sanitization procedure.

Table A-5: Magnetic Media Sanitization

Magnetic Media	
Floppies	
Clear:	Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.
Purge:	Degauss in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate floppy disks and diskettes by burning in a licensed incinerator or Shred.
Magnetic Disks (flexible or fixed)	
Clear:	Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

Purge:	Degauss in an organizationally approved degausser rated at a minimum for the media.
	Incinerate disks and diskettes by burning in a licensed incinerator or Shred.
	Degaussing magnetic disks typically renders the disk permanently unusable.
	Re-record (overwrite) all data on the tape using an organizationally approved pattern, using a system with similar characteristics to the one that originally recorded the data. For example, overwrite previously recorded sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.
	Degauss the magnetic tape in an organizationally approved degausser rated at a minimum for the media.
	Incinerate by burning the tapes in a licensed incinerator or Shred.
	Preparatory steps for Destruction, such as removing the tape from the reel or cassette prior to Destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a Destruction facility or for recycling measures.
	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.
	Four options are available: 1. Use one of the ATA Sanitize Device feature set commands, if supported, to perform a Sanitize operation. One or both of the following options may be available: a. The overwrite EXT command. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. *Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified. b. If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase. 2. Use the ATA Security feature set's SECURE ERASE UNIT command, if support, in Enhanced Erase mode. The ATA Sanitize Device feature set commands are preferred over the over the ATA Security feature set SECURITY ERASE UNIT command when supported by the ATA device. 3. Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface by issuing commands as

	necessary to cause all MEKs to be changed (if the requirements described in this document have been satisfied). Refer to the TCG and device manufacturers for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase. 4. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected. When using the three pass ATA sanitize overwrite procedure with the invert option, the verification process would simply search for the original pattern (which would have been written again during the third pass). The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in section 4.7 should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Given the variability in implementation of the ATA Security feature set SECURITY ERASE UNIT command, use of this command is not recommended without first consulting with the manufacturer to verify that the storage device's model-specific implementation meets the needs of the organization. This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device. Degaussing the media in a storage device typically renders the device unusable.
SCSI Hard Disk Drives *This includes Parallel SCSI,Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express Partial sanitization is not supported in this section.*	
Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may optionally be used.
Purge:	Four options are available: 1. Apply the SCSI SANITIZE command, if supported. One or both of the following options

	may be available: a. The OVERWRITE service action. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. *Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified. b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied. 3. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand. The degausser/wand should be rated sufficient for the media.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected. When using the three pass SCSI sanitize overwrite procedure with the invert (also known as complement) option, the verification process would simply search for the original pattern (which would have been written again during the third pass). While it is widely accepted that one pass of overwriting should be sufficient for Purging the data, the availability of a dedicated command that incorporates the ability to invert the data pattern allows an efficient and effective approach that mitigates any residual risk associated with variations in implementations of magnetic recording features across device manufacturers. The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as "SCSI mode parameter block descriptor's NUMBER OF LOGICAL BLOCKS field (accessible with the SCSI MODE SENSE and MODE SELECT commands". Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device.

	Degaussing the media in a storage device typically renders the device unusable.

Table A-6: Peripherally Attached Storage Sanitization

Peripherally Attached Storage	
External Locally Attached Hard Drives *This includes, USB, Firewire, etc. (Treat eSATA as ATA Hard drive.)*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the issuance of any specific command to the device may not reasonably and consistently assure the desired sanitization result. When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated media-specific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge. Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present.

Table A-7: Optical Media Sanitization

Optical Media	
CD, DVD, BD	
Clear/ Purge:	N/A

Destroy:	Destroy in order of recommendations: 1. Removing the information-bearing layers of CD media using a commercial optical disk grinding device. Note that this applies only to CD and not to DVD or BD media 2. Incinerate optical disk media (reduce to ash) using a licensed facility. 3. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of 0.5 mm and surface area of 0.25 mm^2 or smaller.

Table A-8: Flash Memory-Based Storage Device Sanitization

Flash Memory-Based Storage Devices	
ATA Solid State Drives (SSDs) *This includes PATA, SATA, eSATA, etc.*	
Clear:	1. Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media). 2. Use the ATA Security feature set's SECURITY ERASE UNIT command, if supported.
Purge:	Three options are available: 1. Apply the ATA sanitize command, if supported. One or both of the following options may be available: a. The block erase command. *Optionally:* After the block erase command is successfully applied to a device, write binary 1s across the user addressable area of the storage media and then perform a second block erase. b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.

	The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Given the variability in implementation of the Enhanced Secure Erase feature, use of this command is not recommended without first referring the manufacturer to identify that the storage device's model-specific implementation meets the needs of the organization. Whereas ATA Secure Erase was a Purge mechanism for magnetic media, it is only a Clear mechanism for flash memory due to variability in implementation and the possibility that sensitive data may remain in areas such as spare cells that have been rotated out of use. Degaussing must not be solely relied upon as a sanitization technique on flash memory-based storage devices or on hybrid devices that contain non-volatile flash memory storage media. Degaussing may be used when non-volatile flash memory media is present if the flash memory components are sanitized using media-dependent techniques.
SCSI Solid State Drives (SSSDs) *This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media).
Purge:	Two options are available: 1. Apply the SCSI SANITIZE command, if supported. One or both of the following options may be available: a. The BLOCK ERASE service action. b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as SCSI mode select. Even when a dedicated sanitization

	command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices.
NVM Express SSDs	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	Two options are available: 1. Apply the NVM Express Format command, if supported. One or both of the following options may be available: a. The User Data Erase command. b. If the device supports encryption, the Cryptographic Erase command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data Erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data Erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices.
USB Removable Media *This includes Pen Drives, Thumb Drives, Flash Memory Drives, Memory Sticks, etc.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting

	technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used.
Purge:	Most USB removable media does not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Refer to the manufacturer for details about the availability and functionality of any available sanitization features and commands.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For most cases where Purging is desired, USB removable media should be Destroyed.
Memory Cards *This includes SD, SDHC, MMC, Compact Flash Memory, Microdrive, MemoryStick, etc.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used.
Purge:	N/A
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	None.
Embedded Flash Memory on Boards and Devices *This includes motherboards and peripheral cards such as network adapters or any other adapter containing non volatile flash memory.*	
Clear:	If supported by the device, reset the state to original factory settings.
Purge:	N/A If the flash memory can be easily identified and removed from the board, the flash memory may be Destroyed independently from the disposal of the board that contained the flash memory. Otherwise, the whole board should be Destroyed.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	While Embedded flash memory has traditionally not been specifically addressed in media sanitization guidelines, the increasing complexity of systems and associated use of flash memory has complementarily increased the likelihood that sensitive data may be present. For example, remote management capabilities integrated into a modern motherboard may necessitate storing IP addresses, hostnames, usernames and passwords, certificates, or other data that may be considered sensitive. As a result, for Clearing, it may be necessary to interact with multiple interfaces to fully reset the device state. When this concept is applied to the example, this might include the BIOS/UEFI interface as well as the remote management interface. As with other types of media, the choice of sanitization technique is based on environment-specific considerations. While the choice might be made to neither Clear nor Purge embedded flash memory, it is important to recognize and accept the potential risk and continue to reevaluate the risk as the environment changes.

Table A-9: RAM- and ROM-Based Storage Device Sanitization

RAM and ROM-Based Storage Devices	
Dynamic Random Access Memory (DRAM)	
Clear/ Purge:	Power off device containing DRAM, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device.
Destroy:	Shred, Disintegrate, or Pulverize.
Notes:	In either case, the DRAM must remain without power for a period of at least five minutes.
Electronically Alterable PROM (EAPROM)	
Clear/ Purge:	Perform a full chip Purge as per manufacturer's data sheets.
Destroy:	Shred, Disintegrate, or Pulverize.
Notes:	None.
Electronically Erasable PROM (EEPROM)	
Clear/ Purge:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	None.

Appendix B Glossary

ATA	Magnetic media interface specification. Also known as "IDE" – Integrated Drive Electronics.
BD	A Blu-ray Disc (BD) has the same shape and size as a CD or DVD, but has a higher density and gives the option for data to be multi-layered.
Bend	The use of a mechanical process to physically transform the storage media to alter its shape and make reading the media difficult or infeasible using state of the art laboratory techniques.
Clear	A method of Sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
CD	A Compact Disc (CD) is a class of media from which data are read by optical means.
CD-RW	A Compact Disc Read/Write (CD-RW) is a CD that can be Purged and rewritten multiple times.
CD-R	A Compact Disc Recordable (CD-R) is a CD that can be written on only once but read many times. Also known as WORM.
CE	See *Cryptographic Erase*.
CMRR	The Center for Magnetic Recording Research, located at the University of California, San Diego, advances the state-of-the-art in magnetic storage and trains graduate students and postdoctoral professionals (CMRR homepage: http://cmrr.ucsd.edu/).
Cut	The use of a tool or physical technique to cause a break in the surface of the electronic storage media, potentially breaking the media into two or more pieces and making it difficult or infeasible to recover the data using state of the art laboratory techniques.
Cryptographic Erase	A method of Sanitization in which the Media Encryption Key (MEK) for the encrypted Target Data (or the Key Encryption Key – KEK) is sanitized, making recovery of the decrypted Target Data infeasible.

Data	Pieces of information from which "understandable information" is derived.
Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive. Also called "demagnetizing."
Destroy	A method of Sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.
Digital	The coding scheme generally used in computer technology to represent data.
Disintegration	A physically Destructive method of sanitizing media; the act of separating into component parts.
Disposal	Disposal is a release outcome following the decision that media does not contain sensitive data. This occurs either because the media never contained sensitive data or because Sanitization techniques were applied and the media no longer contains sensitive data.
DVD	A Digital Video Disc (DVD) has the same shape and size as a CD, but with a higher density that gives the option for data to be double-sided and/or double-layered.
DVD-RW	A rewritable (re-recordable) DVD for both movies and data from the DVD Forum.
DVD+RW	A rewritable (re-recordable) DVD for both movies and data from the DVD+RW Alliance.
DVD+R	A write-once (read only) version of the DVD+RW from the DVD+RW Alliance.
DVD-R	A write-once (read only) DVD for both movies and data endorsed by the DVD Forum.
Electronic Media	General term that refers to media on which data are recorded via an electrically based process.
Erasure	Process intended to render magnetically stored information irretrievable by normal means.

FIPS	Federal Information Processing Standard.
Format	Pre-established layout for data.
Hard Disk	A rigid magnetic disk fixed permanently within a drive unit and used for storing data. It could also be a removable cartridge containing one or more magnetic disks.
Incineration	A physically Destructive method of sanitizing media; the act of burning completely to ashes.
Information	Meaningful interpretation or expression of data.
Magnetic Media	A class of storage device that uses only magnetic storage media for persistent storage, without the assistance of heat (ie. heat assisted magnetic recording (HAMR)) or the additional use of other persistent storage media such as flash memory-based media.
Media	Plural of medium.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.
Melting	A physically Destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat.
Optical Disk	A plastic disk that is read using an optical laser device.
Overwrite	Writing data on top of the physical location of data stored on the media.
Physical Destruction	A Sanitization method for media.
Pulverization	A physically Destructive method of sanitizing media; the act of grinding to a powder or dust.
Purge	A method of Sanitization by applying physical or logical techniques that renders Target Data recovery infeasible using state of the art laboratory techniques.
Read	Fundamental process in an information system that results only in the flow of information from storage media to a requester.
Read-Only Memory	ROM is a pre-recorded storage medium that can only be read from

	and not written to.
Record	To write data on a medium, such as a magnetic tape, magnetic disk, or optical disk.
Remanence	Residual information remaining on storage media.
ROM	See *Read-Only Memory*.
Sanitize	A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media.
SANITIZE Command	A command in the ATA and SCSI standards that leverages a firmware-based process to perform a Sanitization action. If a device supports the *sanitize* command, the device must support at least one of three options: *overwrite*, *block erase* (usually for flash memory-based media), or *crypto scramble* (Cryptographic Erase). These commands typically execute substantially faster than attempting to rewrite through the native read and write interface. The ATA standard clearly identifies that the Sanitization operations must address user data areas, user data areas not currently allocated (including "previously allocated areas and physical sectors that have become inaccessible"), and user data caches. The resulting media contents vary based on the command used. The *overwrite* command allows the user to specify the data pattern applied to the media, so that pattern (or the inverse of that pattern, if chosen) will be written to the media (although the actual contents of the media may vary due to encoding). The result of the *block erase* command is vendor unique, but will likely be 0s or 1s. The result of the *crypto scramble* command is vendor unique, but will likely be cryptographically scrambled data (except for areas that were not encrypted, which are set to the value the vendor defines).
SCSI	A magnetic media interface specification. Small Computer System Interface.
Secure Erase Command	An *overwrite* command in the ATA standard (as 'Security Erase Unit') that leverages a firmware-based process to overwrite the media. This command typically executes substantially faster than attempting to rewrite through the native read and write interface. There are up to two options, 'normal erase' and 'enhanced erase'. The normal erase, as defined in the standard, is only required to address data in the contents of LBA 0 through the greater of READ NATIVE MAX or READ NATIVE MAX EXT, and replaces the contents with 0s or 1s. The *enhanced erase* command specifies that, "…all previously written user data shall be overwritten, including

	sectors that are no longer in use due to reallocation" and the contents of the media following Sanitization are vendor unique. The actual action performed by an *enhanced erase* varies by vendor and model, and could include a variety of actions that have varying levels of effectiveness. The *secure erase* command is not defined in the SCSI standard, so it does not apply to media with a SCSI interface.
Shred	A method of sanitizing media; the act of cutting or tearing into small particles.
SSD	A Solid State Drive (SSD) is a storage device that uses solid state memory to store persistent data.
Storage	Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved.
Target Data	The information subject to a given process, typically including most or all information on a piece of storage media.
Validate	The step in the media sanitization process flowchart which involves testing the media to ensure the information cannot be read.
Verification	The process of testing the media to ensure the information cannot be read.
WORM	Write-Once Read Many. Also see *CD-R*.
Write	Fundamental operations of an information system that results only in the flow of information from an actor to storage media.

Appendix C Tools and Resources

Many different government, U.S. military, and academic institutions have conducted extensive research in sanitization tools, techniques, and procedures in order to verify them to a certain level of assurance. NIST does not conduct an evaluation of any tool set to verify its ability to Clear, Purge, or Destroy information contained on any specific medium.

Organizations are encouraged to seek products that they can evaluate on their own. They can use a trusted service or other federal organizations' evaluation of tools and products, and they should continually monitor and verify the effectiveness of their selected sanitization tools as they are used.

If an organization has a product that they trust and have tested, then they are strongly encouraged to share this information through public forums, such as the Federal Computer Security Managers' Forum[22].

C.1 NSA Media Destruction Guidance

This guide also recommends that the user consider the National Security Agency (NSA) devices posted in the Media Destruction Guidance area of the public NSA website[23]. NSA states that "the products on these lists meet specific NSA performance requirements for sanitizing, destroying, or disposing of media containing sensitive or classified information. Inclusion on a list does not constitute an endorsement by NSA or the U.S. Government." The evaluated products lists provided on NSA's website cover:

- Crosscut paper shredders,
- Optical media,
- Degaussers,
- Storage devices, and
- Disintegrators.

C.2 Open Source Tools

There are a variety of open source tools available that support leveraging the sanitize commands based on standardized interfaces. As with any sanitization tool, independent validation should be performed to ensure the desired functionality is provided. However, the availability of open source tools helps organizations understand how the commands work and allows testing of sanitize commands on a drive, as well as supporting the ability of home users to apply sanitization to their personal media.

---

[22] http://csrc.nist.gov/groups/SMA/forum/

[23] http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

For example, one open source project is **hdparm**, which is available on SourceForge[24].

C.3 EPA Information on Electronic Recycling (e-Cycling)

Organizations and individuals wishing to donate used electronic equipment or seeking guidance on disposal of residual materials after sanitization should consult the Environmental Protection Agency's (EPA) electronic recycling and electronic waste information website at http://www.epa.gov/e-Cycling/. This site offers advice, regulations, and standard publications related to sanitization, disposal, and donations. It also provides external links to other sanitization tool resources.

C.4 Outsourcing Media Sanitization and Destruction

Organizations can outsource media sanitization and Destruction if business and security management decide that this would be the most reasonable option for them to maintain confidentiality while optimizing available resources. When exercising this option, this guide recommends that organizations exercise "due diligence" when entering into a contract with another party engaged in media sanitization. Due diligence for this case is accepted as outlined in 16 CFR 682 which states "due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule [guide], obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.'[25]

C.5 Trusted Computing Group Storage Specifications

Information on the TCG storage specifications (Opal SSC or Enterprise SSC interface specs) is available on the TCG's website:
http://www.trustedcomputinggroup.org/

C.6 Standards for ATA and SCSI

Information on the ATA and SCSI standards is available at:

http://www.t13.org/

http://www.t10.org/

Note: The ATA and SCSI standards are published by:

---

[24] http://hdparm.sourceforge.net/

[25] "Disposal of Consumer Report Information and Records Section," Title 16 *Code of Federal Regulations*, Pt. 682.3 (b) (3).

a) INCITS and ANSI as an American National Standard (see http://www.incits.org and http://www.ansi.org)

b) ISO/IEC as an International standard (see http://www.iso.org and http://www.iec.ch)

C.7 NVM Express Specification

Information on NVM Express is available at:

http://www.nvmexpress.org/

Appendix D Cryptographic Erase Device Guidelines

The determination of whether to use Cryptographic Erase on a given device depends on an organization's sanitization requirements. It also depends on the end user's ability to determine whether the implementation offers sufficient assurance against future recovery of the data. The level of assurance depends in large part on the factors described in Table D-1.

Table D-1: Cryptographic Erase Considerations

Area	Consideration(s)	Relevant Doc(s)
Key Generation	The level of entropy of the random number sources and quality of whitening procedures applied to the random data. This applies to the cryptographic keys, and potentially to wrapping keys affected by the CE operation.	SP 800-90[26] SP 800-90A SP 800-90B SP 800-90C, SP 800-133
Media Encryption	The security strength and validity of implementation of the encryption algorithm/mode used for protection of the Target Data.	FIPS 140-2[27] FIPS 197 SP 800-38A (not including ECB) SP 800-38E
Key Level and Wrapping	The key being sanitized might not be the Media Encryption Key (MEK), but instead a key used to wrap (that is, encrypt) the MEK or another key. In this case, the security strength and level of assurance of the wrapping techniques used should be commensurate with the level of strength of the CE operation.	FIPS 197 SP 800-38A SP 800-38F SP 800-131A

Before relying on Cryptographic Erase for media sanitization, users should identify the mechanisms implemented by the storage device to address these areas:

1. **Make/Model/Version/Media Type:** The product and versions the statement applies to, and the type of media the device uses (ie. magnetic, SSD, hybrid, other).

   Many devices store the Target Data in several different media - e.g. a DRAM (Dynamic Random Access Memory) cache in addition to rotating platters. It is important to identify the storage locations and how each is sanitized.

[26] A list of validated Deterministic Random Bit Generators (DRBGs) is available at: http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html.

[27] Conformance testing for FIPS 140-2 is conducted within the framework of the Cryptographic Module Validation Program (CMVP), http://csrc.nist.gov/groups/STM/cmvp/, and the Cryptographic Algorithm Validation Program (CAVP), http://csrc.nist.gov/groups/STM/cavp/.

2. **Key Generation:** Identify whether a Deterministic Random Bit Generator (DRBG), such as one of those listed in SP 800-90,[28] was used, and whether it was validated.

3. **Media Encryption:** Identify the algorithm, key strength, mode of operation, and any applicable validation(s).

4. **Key Level and Wrapping:** Identify if the MEK (either wrapped with another value or not wrapped) is directly sanitized, or if a key that wraps the MEK (a key encryption key, or KEK) is sanitized. A description of the wrapping techniques only applies where a KEK (and not the MEK) is sanitized. Wrapping details, when provided, should include the algorithm used, strength, and (if applicable) mode of operation.

5. **Data Areas Addressed:** Describe which areas are encrypted and which areas are not encrypted. For any unencrypted areas, describe how sanitization is performed.

6. **Key Life Cycle Management:** The key(s) on a device may have multiple wrapping activities (wrapping, unwrapping, and rewrapping) throughout the device's lifecycle. Identify how the key(s) being sanitized are handled during wrapping activities that are not directly part of the Cryptographic Erase operation. For example, a user may have received an SED that was always encrypting, and simply turned on the authentication interface. Identify how the previous instance of the MEK was sanitized when it was wrapped with the user's authentication credentials.

7. **Key Sanitization Technique:** Describe the media-dependent sanitization method for the key being sanitized. Some examples might include one or more inverted overwrite passes if the media is magnetic, a block erase for an SSD, or other media-specific techniques for other types of media.

8. **Key Escrow or Backup:** Identify whether the device supports key escrow or backup. Identify whether the device supports discovery of whether any key(s) at or below the level of the key escrowed has/have ever been escrowed from or injected into the device.If the MEK is directly sanitized and only a KEK can be escrowed, clearly identify that fact.

9. **Error Condition Handling:** Identify how the device handles error conditions that prevent the Cryptographic Erase operation from fully completing. For example, if the location where the key was stored cannot be sanitized, does the Cryptographic Erase operation report success or failure to the user?

10. **Interface Clarity:** Identify which interface commands support the features described in the statement. If the device supports the use of multiple MEKs, identify whether all MEKs are changed using the interface commands available and any additional commands or actions necessary to ensure all MEKs are changed. Note that under certain conditions, not all MEKs have to be cleared (e.g., partial sanitization of target data).

[28] NIST SP 800-90A (as amended), *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012, 136 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

D.1 Example Statement of Cryptographic Erase Features

The following statements should be placed by the storage device vendor in an area accessible to potential users of a device, such as on the vendor's website or in product literature that is widely available. Information of a proprietary nature may not be available in published product information.

1. **Make/Model/Version/Media Type:** Acme hard drive model abc12345 version 1+. Media type is Legacy Magnetic media.

2. **Key Generation:** A DRBG is used as specified in SP 800-90, with validation [number].

3. **Media Encryption:** Media is encrypted with AES-256 media encryption in Cipher Block Chaining (CBC) mode as described in SP 800-38A. This device is FIPS 140 validated with certificate [number].

4. **Key Level and Wrapping:** The media encryption key is sanitized directly during Cryptographic Erase.

5. **Data Areas Addressed:** The device encrypts all data stored in the LBA-addressable space except for a preboot authentication and variable area and the device logs. Device log data is retained by the device following Cryptographic Erase.

6. **Key Lifecycle Management:** As the MEK moves between wrapped, unwrapped, and re-wrapped states, the previous instance is sanitized using three inverted overwrite passes.

7. **Key Sanitization Technique:** Three passes with a pattern that is inverted between passes.

8. **Key Escrow or Injection:** The device does not support escrow or injection of the keys at or below the level of the sanitization operation.

9. **Error Condition Handling:** If the storage device encounters a defect in a location where a key is stored, the device attempts to rewrite the location and the Cryptographic Erase operations continues, reporting success to the user if the operation is otherwise successful.

10. **Interface Clarity:** The device has an ATA interface and supports the ATA Sanitize Device feature set CRYPTO SCRAMBLE EXT command and a TCG Opal interface with the ability to sanitize the device by cryptographically erasing the contents. Both of these commands apply the functionality described in this statement.

Appendix E Device Specific Characteristics of Interest

Storage vendors implement a range of devices and media types that leverage the same standardized command sets. Some examples of command sets include ATA, SCSI, and NVM Express. There are likely to be differences in implementation between, for example, the enhanced Security Erase command for ATA devices from different vendors. Some vendors may have implementations 'under the hood' that apply techniques such as Cryptographic Erase, block erase (for flash memory devices), or other techniques. It may be difficult or impossible for users to know for sure how the sanitization action is being implemented.

In order to support informed decision making by users, vendors may choose to provide information about how a specific device implements any dedicated sanitize commands supported by the device. When reported by vendors, this information also helps purchasing authorities make informed decisions about which storage devices to acquire based on the availability of suitable sanitization functions and approaches. This vendor-reported information should address the following:

- The media type (i.e., Legacy Magnetic, HAMR, magnetic shingle, SLC/MLC/TLC Flash Memory, Hybrid, etc.)
    - If the device contains magnetic media, the coercivity of the magnetic media (to support an informed decision about whether to attempt to degauss the media)
- Which sanitize commands are supported (if any)
- For each sanitize command supported:
    - A list of any areas not addressed by the sanitization command
    - The estimated time necessary for the command to successfully complete
    - The results of any validation testing, if applicable

Appendix F Selected Bibliography

Additional sources of useful information pertinent to SP 800-88 Rev 1

- *All About Degaussers and Erasure of Magnetic Media*, Athana International [Web page], http://www.athana.com/ddequip/allaboutdegaussers.htm [accessed 7/18/14].
- J. Anastasi, *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property.* Hoboken, N.J.: John Wiley and Sons, 2003.
- J. Daughton, *Magnetoresistive Random Access Memory (MRAM)*, (February 4, 2000), 13pp. http://www.nve.com/Downloads/mram.pdf [accessed 7/21/14].
- H.A. Davis, National Security Agency. NSA/CSS POLICY MANUAL 9-12. (NSA/CSS STORAGE DEVICE DECLASSIFICATION MANUAL) http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf N.p.: n.p., 2006.
- *Degaussing Described.* Weircliffe International Ltd, 9th English edition, 2006. Archived copy available at: https://web.archive.org/web/20070129044258/http://www.weircliffe.co.uk/pdf/Weircliffe_Degaussing.pdf [accessed 7/18/14]..
- Y. Deng, "What is the future of disk drives, death or rebirth?" *ACM Computing Surveys*, 43(3), Article no. 23, (April 2011). http://dx.doi.org/10.1145/1922649.1922660.
- S.L. Garfinkel, and A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security & Privacy* 1(1), 17-27, (Jan.-Feb. 2003). http://dx.doi.org/10.1109/MSECP.2003.1176992.
- G. Gibson, and M. Polte, *Directions for Shingled-Write and Two- Dimensional Magnetic Recording System Architectures: Synergies with Solid-State Disks*, CMU-PDL-09-104, Carnegie Mellon University Parallel Data Laboratory, Pittsburgh, Pennsylvania, May 2009, 2pp. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=pdl [accessed 7/21/14].
- *A Guide to Understanding Data Remanence in Automated Information Systems*, National Computer Security Center, NCSC-TG-025, Version 2. https://www.marcorsyscom.usmc.mil/Sites/PMIA%20Documents/Resources/national/NCSC-TG-025%20Data%20Remanence.html [accessed 7/21/14].
- P. Gutmann, "Data Remanence in Semiconductor Devices," *Proceedings of the 10th USENIX Security Symposium*, Washington, D.C. (August 13-17, 2001), 16pp. http://static.usenix.org/publications/library/proceedings/sec01/full_papers/gutmann/gutmann.pdf [accessed 7/21/14].
- P. Gutmann, , "Secure Deletion of Data from Magnetic and Solid-State Memory," *Proceedings of the Sixth USENIX Security Symposium*, San Jose, California, (July 22-25,

1996) 77-90. http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html [accessed 7/21/14].

- G.F. Hughes, T. Coughlin, T., and D.M. Commins, "Disposal of Disk and Tape Data by Secure Sanitization," *IEEE Security & Privacy* 7(4), 29-34 (July-Aug. 2009). http://dx.doi.org/10.1109/MSP.2009.89.

- InterNational Committee for Information Technology Standards. *Information technology – AT Attachment 8 - ATA/ATAPI Command Set - 2 (ATA8-ACS-2)*, INCITS 482-2012, American National Standards Institute, New York, May 30, 2012.

- InterNational Committee for Information Technology Standards., *Information technology - SCSI Primary Commands - 4 (SPC-4)*, INCITS 513, May 17, 2014. http://www.t10.org/cgi-bin/ac.pl?t=f&f=spc4r37.pdf [accessed 7/18/14].

- J. Hasson, "V.A. Toughens Security after PC Disposal Blunders," *Federal Computer Week*, August 26, 2002. http://fcw.com/Articles/2002/08/26/VA-toughens-security-after-PC-disposal-blunders.aspx [accessed 7/21/14].

- C. King, and T. Vidas, "Empirical analysis of solid state disk data retention when used with contemporary operating systems," *Digital Investigation* 8 (2011), S111-S117. http://dx.doi.org/10.1016/j.diin.2011.05.013.

- *Microsoft EFI FAT32 File System Specification*, Microsoft Corporation, December 6, 2000. http://msdn.microsoft.com/en-us/library/windows/hardware/gg463080.aspx [accessed 7/21/14].

- B.J. Phillips, C.D. Schmidt, and D.R. Kelly, "Recovering data from USB flash memory sticks that have been damaged or electronically erased," *e-Forensics '08: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, Adelaide, Australia (January 21-23, 2008), article no. 19. http://dx.doi.org/10.4108/e-forensics.2008.2771.

- A. Suresh, G. Gibson, and G. Ganger. *Shingled Magnetic Recording for Big Data Applications*, CMU-PDL-12-105, Carnegie Mellon University, Parallel Data Lab, Pittsburgh, Pennsylvania, May 2012, 29 pp. http://www.pdl.cmu.edu/PDL-FTP/FS/CMU-PDL-12-105.pdf [accessed 7/18/14].

- U.S. Army. *Information Assurance*, Army Regulation (AR) 25–2, October 24, 2007 (with Rapid Action Release on March 23, 2009). http://armypubs.army.mil/epubs/pdf/r25_2.pdf [accessed 7/18/14].

- U.S. Department of Defense, "Clearing and Sanitization Data Storage," Table C8.T1 in *National Industrial Security Program: Operating Manual*, DoD 5220.22-M-Sup-1, Washington, D.C. (February 1, 2005), pp.82-83. http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf Page 81[accessed 7/21/14].

- *Understand Degaussing*, Peripheral Manufacturing Inc. [Web page], http://www.periphman.com/understand_degaussing.shtml [accessed 7/21/14].

- M. Wei, L.M. Grupp, F.E. Spada, and S. Swanson, "Reliably Erasing Data From Flash-Based Solid State Drives," *9th USENIX Conference on File and Storage Technologies (FAST '11)*, San Jose, California (February 15-17, 2011), 13pp. http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf [accessed 7/21/14].

- B. Xu, J. Yang, H. Yuan, J. Zhang, Q. Zhang, and T.C. Chong, "Thermal Effects in Heat Assisted Bit Patterned Media Recording," *IEEE Transactions on Magnetics* 45(5) 2292-2295 (May 2009). http://dx.doi.org/10.1109/TMAG.2009.2016466.

Appendix G Sample "Certificate of Sanitization" Form

This certificate is simply an example to demonstrate the types of information that should be collected and how a certificate might be formatted. An organization could alternatively choose to electronically record sanitization details, either through a native application or by using a form such as this one with an automated data transfer utility (such as a PDF form with a button to send the data to a database or email address). In the event that the records need to be referenced in the future, electronic records will likely provide the fastest search capabilities and best likelihood that the records are reliably retained.

CERTIFICATE OF SANITIZATION		
PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITIZATION DETAILS		
Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct		
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other:		
Method Details:		
Tool Used *(include version):*		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)*		
Details:		
SIGNATURE		
I attest that the information provided on this statement is accurate to the best of my knowledge.		
Signature:		Date:
VALIDATION		
Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date:

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

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

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

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

MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

February 2020
INCLUDES UPDATES AS OF 01-28-2021; SEE PAGE X

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

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

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, 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, Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-171, Revision 2, **113 pages** (February 2020)

CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

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

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

Comments on this publication may be submitted to:

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

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96]

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) 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 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 privacy and its collaborative activities with industry, government, and academic organizations.

Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Keywords

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

Acknowledgements

The authors wish to recognize the scientists, engineers, and research staff from the Computer Security Division and Applied Cybersecurity Division for their exceptional contributions in helping to improve the content of the publication. A special note of thanks to Pat O'Reilly, Jim Foti, Jeff Brewer and the NIST web team for their outstanding administrative support. Finally, the authors also gratefully acknowledge the contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

HISTORICAL CONTRIBUTIONS TO NIST SPECIAL PUBLICATION 800-171

The authors acknowledge the many individuals who contributed to previous versions of Special Publication 800-171 since its inception in June 2015. They include Carol Bales, Matthew Barrett, Jon Boyens, Devin Casey, Christian Enloe, Peggy Himes, Robert Glenn, Elizabeth Lennon, Vicki Michetti, Dorian Pappas, Karen Quigg, Mary Thomas, Matthew Scholl, Murugiah Souppaya, Patricia Toth, and Patrick Viscuso.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

CAUTIONARY NOTE

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

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

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

CUI SECURITY REQUIREMENTS

The recommended security requirements contained in this publication are only *applicable* to a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement. The security requirements apply to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

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

ADDITIONAL RESOURCES

Mapping security controls to the Cybersecurity Framework: https://csrc.nist.gov/publications/detail/nistir/8170/draft.

Mapping CUI security requirements to the Cybersecurity Framework: https://csrc.nist.gov/projects/cybersecurity-framework/informative-reference-catalog/details/1.

Table of Contents

Errata

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

DATE	TYPE	CHANGE	PAGE
01-28-2021	Editorial	Front Matter Blue Box: Change “The requirements apply only” to “The security requirements apply"	vii
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 1: Delete: “The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.”	2
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 2: Add “The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization’s security posture to a level beyond that which it requires for protecting its missions, operations, and assets.”	2
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 3: Change: “The requirements are“ to “The recommended security requirements in this publication are”	3
01-28-2021	Editorial	Chapter One, Section 1.1, Paragraph 6: Delete: “If nonfederal organizations entrusted with protecting CUI designate systems or components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements to only those systems or components. Isolating CUI into its own security domain by applying architectural design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices) may be the most cost-effective and efficient approach for nonfederal organizations to satisfy the security requirements and protect the confidentiality of CUI. Security domains may employ physical separation, logical separation, or a combination of both. This approach can reasonably provide adequate security for the CUI and avoid increasing the organization’s security posture to a level beyond which it typically requires for protecting its missions, operations, and assets.”	4

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 information systems.[1] Many federal contractors process, store, and transmit sensitive federal information to support the delivery of essential products and services to federal agencies (e.g., providing financial services; providing web and electronic mail services; processing security clearances or healthcare data; providing cloud services; and developing communications, satellite, and weapons systems). Federal information is frequently provided to or shared with entities such as state and local governments, colleges and universities, and independent research organizations. The protection of sensitive federal information while residing in *nonfederal systems*[2] and organizations is of paramount importance to federal agencies, and can directly impact the ability of the federal government to carry out its designated missions and business operations.

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies. [EO 13556] established a governmentwide Controlled Unclassified Information (CUI)[3] 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 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 [NARA CUI]. The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent. The CUI Registry identifies approved CUI categories, 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, reusing, and disposing of the information.

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

[2] A *federal information system* is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. A system that does not meet such criteria is a *nonfederal system*.

[3] *Controlled Unclassified Information* is any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under [EO 13526] or any predecessor or successor order, or [ATOM54], as amended.

[4] [EO 13556] designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the CUI Program.

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

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide federal agencies with recommended security requirements[6] for protecting the *confidentiality* of CUI: (1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[7] and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.[8]

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.[9] If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

[5] [32 CFR 2002] was issued on September 14, 2016 and became effective on November 14, 2016.

[6] The term *requirements* can be used in different contexts. In the context of federal information security and privacy policies, the term is generally used to refer to information security and privacy obligations imposed on organizations. For example, OMB Circular A-130 imposes a series of information security and privacy requirements with which federal agencies must comply when managing information resources. In addition to the use of the term requirements in the context of federal policy, the term requirements is used in this guideline in a broader sense to refer to an expression of the set of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and corresponding security requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). The term requirements, as used in this guideline, includes both legal and policy requirements, as well as an expression of the broader set of stakeholder protection needs that may be derived from other sources. All of these requirements, when applied to a system, help determine the required characteristics of the system.

[7] Nonfederal organizations that collect or maintain information *on behalf of* a federal agency or that use or operate a system *on behalf of* an agency, must comply with the requirements in [FISMA], including the requirements in [FIPS 200] and the security controls in [SP 800-53] (See [44 USC 3554] (a)(1)(A)).

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

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

The recommended security requirements in this publication are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR),[10] the CUI Executive Agent will address determining compliance with security requirements.[11]

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

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality);[12]
- 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*.

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

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

[10] NARA, as the CUI Executive Agent, plans to sponsor a single FAR clause that will apply the requirements of the federal CUI regulation and NIST Special Publication 800-171 to contractors. Until the FAR clause is in place, the requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

[11] [SP 800-171A] provides assessment procedures to determine compliance to the CUI security requirements.

[12] [FIPS 199] defines three values of potential impact (i.e., low, moderate, high) on organizations, assets, or individuals in the event of a breach of security (e.g., a loss of confidentiality).

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

requirements to protect CUI Basic[14] at higher than moderate confidentiality. The provision of safeguarding requirements for CUI in a specified category will be addressed by the National Archives and Records Administration (NARA) in its CUI guidance and in the CUI FAR; and reflected as specific requirements in contracts or other agreements. Nonfederal organizations may use the same CUI infrastructure for multiple government contracts or agreements, if the CUI infrastructure meets the safeguarding requirements for the organization's CUI-related contracts and/or agreements including any specific safeguarding required or permitted by the authorizing law, regulation, or governmentwide policy.

1.2 TARGET AUDIENCE

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

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators);
- Acquisition or procurement responsibilities (e.g., contracting officers);
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers); and
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

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

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

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

[14] CUI Basic is defined in the CUI Registry [NARA CUI].

CHAPTER TWO

THE FUNDAMENTALS

ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING SECURITY REQUIREMENTS

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

2.1 BASIC ASSUMPTIONS

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

- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations; and
- The confidentiality impact value for CUI is no less than [FIPS 199] *moderate*.[15] [16]

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

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

[15] The moderate impact *value* defined in [FIPS 199] may become part of a moderate impact *system* in [FIPS 200], which requires the use of the moderate baseline in [SP 800-53] as the starting point for tailoring actions.

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

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

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

2.2 DEVELOPMENT OF SECURITY REQUIREMENTS

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

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.[17]

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 moderate baseline based on the CUI tailoring criteria described above.

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 systems and organizations. Appendix D provides informal mappings of the security requirements to the relevant security controls in [SP 800-53] and [ISO 27001]. The mappings promote a better understanding of the CUI security requirements, and are *not* intended to impose additional requirements on nonfederal organizations.

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

The following *Media Protection* family example illustrates the structure of a CUI requirement:

Basic Security Requirements

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

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

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

Derived Security Requirements

3.8.4 Mark media with necessary CUI markings and distribution limitations.

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

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

3.8.7 Control the use of removable media on system components.

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

3.8.9 Protect the confidentiality of backup CUI at storage locations.

For ease of use, the security requirements are organized into fourteen *families*. Each family contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum-security requirements for federal information and systems described in [FIPS 200]. The *contingency planning*, *system and services acquisition*, and *planning* requirements are not included within the scope of this publication due to the tailoring criteria.[18] 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

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

A *discussion* section follows each CUI security requirement providing additional information to facilitate the implementation and assessment of the requirements. This information is derived primarily from the security controls discussion sections in [SP 800-53] and is provided to give organizations a better understanding of the mechanisms and procedures used to implement the controls used to protect CUI. The discussion section is *informative*, not *normative*. It is not intended to extend the scope of a requirement or to influence the solutions organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive, and not reflective of potential options available to organizations. Figure 1 illustrates basic security requirement 3.8.3 with its supporting discussion section and informative references.

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

DISCUSSION

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

[SP 800-88] provides guidance on media sanitization.

FIGURE 1: FORMAT AND STRUCTURE OF CUI SECURITY REQUIREMENT

CHAPTER THREE

THE REQUIREMENTS

SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

This chapter describes fourteen families of recommended security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.[19] The security controls from [SP 800-53] associated with the basic and derived requirements are listed in Appendix D.[20] Organizations can use the NIST publication to obtain additional, non-prescriptive information related to the recommended security requirements (e.g., explanatory information in the discussion section for each of the referenced security controls, mapping tables to [ISO 27001] security controls, and a catalog of optional controls that can be used to specify additional security requirements, if needed). This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.[21]

DISCUSSION SECTION

The discussion section associated with each CUI requirement is *informative*, not *normative*. It is not intended to extend the scope of a requirement or to influence the solutions organizations may use to satisfy a requirement. In addition, the use of examples is notional, not exhaustive, and not reflective of potential options available to organizations.

Nonfederal organizations describe, in a system security plan, how the security requirements are met or how organizations plan to meet the requirements and address known and anticipated threats. The system security plan describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and the plan of action as separate or combined documents and in any chosen format.[22]

[19] The security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms at the system level support both objectives. Therefore, the basic and derived security requirements in this publication provide protection from unauthorized disclosure and unauthorized modification of CUI.

[20] The security control references in Appendix D are included to promote a better understanding of the recommended security requirements and do not expand the scope of the requirements.

[21] To promote consistency, transparency, and comparability, the compensatory security measures selected by organizations are based on or derived from *existing* and *recognized* security standards and control sets, including, for example, [ISO 27001] or [SP 800-53].

[22] [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for system security plans and plans of action.

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

The recommended security requirements in this publication apply only to the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. Some systems, including specialized systems (e.g., industrial/process control systems, medical devices, Computer Numerical Control machines), may have limitations on the application of certain security requirements.

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

THE MEANING OF ORGANIZATIONAL SYSTEMS

The term *organizational system* is used in many of the recommended CUI security requirements in this publication. This term has a specific meaning regarding the scope of applicability for the security requirements. The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components. The appropriate scoping for the CUI security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

3.1 ACCESS CONTROL

Basic Security Requirements

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

DISCUSSION

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.

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

DISCUSSION

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Derived Security Requirements

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

DISCUSSION

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: 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 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.

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

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

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

DISCUSSION

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

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

DISCUSSION

Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

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

DISCUSSION

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

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

DISCUSSION

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

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

3.1.8 Limit unsuccessful logon attempts.

DISCUSSION

This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the

organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

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

DISCUSSION

System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

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

DISCUSSION

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

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

DISCUSSION

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

3.1.12 Monitor and control remote access sessions.

DISCUSSION

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with

appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

[SP 800-46], [SP 800-77], and [SP 800-113] provide guidance on secure remote access and virtual private networks.

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

DISCUSSION

Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; [NIST CMVP]; National Security Agency Cryptographic Standards.

3.1.14 Route remote access via managed access control points.

DISCUSSION

Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

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

DISCUSSION

A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

3.1.16 Authorize wireless access prior to allowing such connections.

DISCUSSION

Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

[SP 800-97] provide guidance on secure wireless networks.

3.1.17 Protect wireless access using authentication and encryption.

DISCUSSION

Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See [NIST CRYPTO].

3.1.18 Control connection of mobile devices.

DISCUSSION

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

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements.

[SP 800-124] provides guidance on mobile device security.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.[23]

DISCUSSION

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

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

DISCUSSION

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If

[23] Mobile devices and computing platforms include, for example, smartphones and tablets.

terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

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

DISCUSSION

Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

3.1.22 **Control CUI posted or processed on publicly accessible systems.**

DISCUSSION

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

3.2 AWARENESS AND TRAINING

Basic Security Requirements

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

DISCUSSION

Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security

incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

[SP 800-50] provides guidance on security awareness and training programs.

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

DISCUSSION

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

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

[SP 800-181] provides guidance on role-based information security training in the workplace. [SP 800-161] provides guidance on supply chain risk management.

Derived Security Requirements

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

DISCUSSION

Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements

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

DISCUSSION

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).

Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making.

[SP 800-92] provides guidance on security log management.

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

DISCUSSION

This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of Voice over Internet Protocol (VoIP).

Derived Security Requirements

3.3.3 Review and update logged events.

DISCUSSION

The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

3.3.4 Alert in the event of an audit logging process failure.

DISCUSSION

Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

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

DISCUSSION

Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

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

DISCUSSION

Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

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

DISCUSSION

Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network. See [IETF 5905].

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

DISCUSSION

Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.

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

DISCUSSION

Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

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

DISCUSSION

Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include manufacturer, device type, model, serial number, and physical location.

[SP 800-128] provides guidance on security-focused configuration management.

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

DISCUSSION

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and 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 parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.

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 system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

[SP 800-70] and [SP 800-128] provide guidance on security configuration settings.

Derived Security Requirements

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

DISCUSSION

Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.

[SP 800-128] provides guidance on configuration change control.

3.4.4 Analyze the security impact of changes prior to implementation.

DISCUSSION

Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

[SP 800-128] provides guidance on configuration change control and security impact analysis.

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

DISCUSSION

Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries.

Access restrictions include physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during certain specified times). In addition to security concerns, commonly-accepted due diligence for configuration management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration.

[SP 800-128] provides guidance on configuration change control.

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

DISCUSSION

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

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

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

DISCUSSION

Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.

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

DISCUSSION

The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

[SP 800-167] provides guidance on application whitelisting.

3.4.9 Control and monitor user-installed software.

DISCUSSION

Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved "app stores." Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements

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

DISCUSSION

Common device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

[SP 800-63-3] provides guidance on digital identities.

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

DISCUSSION

Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

[SP 800-63-3] provides guidance on digital identities.

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.**[24] [25]

DISCUSSION

Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security.

Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.

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

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

[SP 800-63-3] provides guidance on digital identities.

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

DISCUSSION

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

[SP 800-63-3] provides guidance on digital identities.

3.5.5 Prevent reuse of identifiers for a defined period.

DISCUSSION

Identifiers are provided for users, processes acting on behalf of users, or devices (3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

3.5.6 Disable identifiers after a defined period of inactivity.

DISCUSSION

Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.

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

DISCUSSION

This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

3.5.8 Prohibit password reuse for a specified number of generations.

DISCUSSION

Password lifetime restrictions do not apply to temporary passwords.

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

DISCUSSION

Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

3.5.10 Store and transmit only cryptographically-protected passwords.

DISCUSSION

Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords. See [NIST CRYPTO].

3.5.11 Obscure feedback of authentication information.

DISCUSSION

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

3.6 INCIDENT RESPONSE

Basic Security Requirements

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

DISCUSSION

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

[SP 800-61] provides guidance on incident handling. [SP 800-86] and [SP 800-101] provide guidance on integrating forensic techniques into incident response. [SP 800-161] provides guidance on supply chain risk management.

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

DISCUSSION

Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies.

[SP 800-61] provides guidance on incident handling.

Derived Security Requirements

3.6.3 **Test the organizational incident response capability.**

DISCUSSION

Organizations test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

[SP 800-84] provides guidance on testing programs for information technology capabilities.

3.7 MAINTENANCE

Basic Security Requirements

3.7.1 **Perform maintenance on organizational systems.**[26]

DISCUSSION

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

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

DISCUSSION

This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the

[26] 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.

controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

Derived Security Requirements

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

DISCUSSION

This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement).

[SP 800-88] provides guidance on media sanitization.

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

DISCUSSION

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

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

DISCUSSION

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

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

DISCUSSION

This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

3.8 MEDIA PROTECTION

Basic Security Requirements

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

DISCUSSION

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

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

[SP 800-111] provides guidance on storage encryption technologies for end user devices.

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

DISCUSSION

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

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

DISCUSSION

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

[SP 800-88] provides guidance on media sanitization.

Derived Security Requirements

3.8.4 **Mark media with necessary CUI markings and distribution limitations.**[27]

DISCUSSION

The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. See [NARA MARK].

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

DISCUSSION

Controlled areas are areas or spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information. Controls to maintain accountability for media during transport include locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

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.**

DISCUSSION

This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). See [NIST CRYPTO].

[SP 800-111] provides guidance on storage encryption technologies for end user devices.

3.8.7 **Control the use of removable media on system components.**

DISCUSSION

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

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable

[27] The implementation of this requirement is per marking guidance in [32 CFR 2002] and [NARA CUI]. Standard Form (SF) 902 (approximate size 2.125" x 1.25") and SF 903 (approximate size 2.125" x .625") can be used on media that contains CUI such as hard drives, or USB devices. Both forms are available from https://www.gsaadvantage.gov. SF 902: NSN 7540-01-679-3318. SF 903: NSN 7540-01-679-3319.

storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices.

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

DISCUSSION

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

3.8.9 Protect the confidentiality of backup CUI at storage locations.

DISCUSSION

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

3.9 PERSONNEL SECURITY

Basic Security Requirements

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

DISCUSSION

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

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

DISCUSSION

Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions

within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Derived Security Requirements

None.

3.10 PHYSICAL PROTECTION

Basic Security Requirements

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

DISCUSSION

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

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

DISCUSSION

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

Derived Security Requirements

3.10.3 **Escort visitors and monitor visitor activity.**

DISCUSSION

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

3.10.4 **Maintain audit logs of physical access.**

DISCUSSION

Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

3.10.5 **Control and manage physical access devices.**

DISCUSSION

Physical access devices include keys, locks, combinations, and card readers.

3.10.6 **Enforce safeguarding measures for CUI at alternate work sites.**

DISCUSSION

Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

[SP 800-46] and [SP 800-114] provide guidance on enterprise and user security when teleworking.

3.11 RISK ASSESSMENT

Basic Security Requirements

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

DISCUSSION

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

[SP 800-30] provides guidance on conducting risk assessments.

Derived Security Requirements

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

DISCUSSION

Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static

analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

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

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

[SP 800-40] provides guidance on vulnerability management.

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

DISCUSSION

Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

3.12 SECURITY ASSESSMENT

Basic Security Requirements

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

DISCUSSION

Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

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

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

[SP 800-53] provides guidance on security and privacy controls for systems and organizations. [SP 800-53A] provides guidance on developing security assessment plans and conducting assessments.

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

DISCUSSION

The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization. [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for plans of action.

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

DISCUSSION

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions.

Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

[SP 800-137] provides guidance on continuous monitoring.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.[28]

DISCUSSION

System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls.

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

System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

[SP 800-18] provides guidance on developing security plans. [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for system security plans.

Derived Security Requirements

None.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements

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

DISCUSSION

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

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

[SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

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

DISCUSSION

Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security

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

[SP 800-160-1] provides guidance on systems security engineering.

Derived Security Requirements

3.13.3 Separate user functionality from system management functionality.

DISCUSSION

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

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

DISCUSSION

The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

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

DISCUSSION

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies.

[SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

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

DISCUSSION

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

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

DISCUSSION

Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

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

DISCUSSION

This requirement applies to internal and external networks and any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of the controls for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted. See [NIST CRYPTO].

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

DISCUSSION

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include de-allocating associated TCP/IP address or port

pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of user inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

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

DISCUSSION

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

[SP 800-56A] and [SP 800-57-1] provide guidance on cryptographic key management and key establishment.

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

DISCUSSION

Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; and [NIST CMVP].

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29]

DISCUSSION

Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

3.13.13 Control and monitor the use of mobile code.

DISCUSSION

Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source.

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

[SP 800-28] provides guidance on mobile code.

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

DISCUSSION

VoIP has different requirements, features, functionality, availability, and service limitations when compared with the Plain Old Telephone Service (POTS) (i.e., the standard telephone service). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

[SP 800-58] provides guidance on Voice Over IP Systems.

3.13.15 Protect the authenticity of communications sessions.

DISCUSSION

Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

[SP 800-77], [SP 800-95], and [SP 800-113] provide guidance on secure communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

DISCUSSION

Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. See [NIST CRYPTO].

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements

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

DISCUSSION

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness

Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.

[SP 800-40] provides guidance on patch management technologies.

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

DISCUSSION

Designated locations include system entry and exit points which may include firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

[SP 800-83] provides guidance on malware incident prevention.

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

DISCUSSION

There are many publicly available sources of system security alerts and advisories. For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations

[SP 800-161] provides guidance on supply chain risk management.

Derived Security Requirements

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

DISCUSSION

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

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

DISCUSSION

Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

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

DISCUSSION

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised

systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[SP 800-94] provides guidance on intrusion detection and prevention systems.

3.14.7 Identify unauthorized use of organizational systems.

DISCUSSION

System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs.

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

[SP 800-94] provides guidance on intrusion detection and prevention systems.

APPENDIX A

REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES[30]

LAWS AND EXECUTIVE ORDERS	
[ATOM54]	Atomic Energy Act (P.L. 83-703), August 1954. https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/app/details/PLAW-104publ231
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[40 USC 11331]	Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331
[44 USC 3502]	Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
[44 USC 3554]	Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3554
[EO 13526]	Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009. https://www.govinfo.gov/app/details/DCPD-200901022
[EO 13556]	Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010. https://www.govinfo.gov/app/details/DCPD-201000942
POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS	
[32 CFR 2002]	32 CFR Part 2002, Controlled Unclassified Information, September 2016. https://www.govinfo.gov/app/details/CFR-2017-title32-vol6/CFR-2017-title32-vol6-part2002/summary

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

[OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[CNSSI 4009] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

STANDARDS, GUIDELINES, AND REPORTS

[ISO 27001] International Organization for Standardization/International Electrotechnical Commission (2013) Information Technology—Security techniques— Information security management systems—Requirements. (International Organization for Standardization, Geneva, Switzerland), ISO/IEC 27001:2013. https://www.iso.org/standard/54534.html

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-28] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-40] Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[SP 800-41] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1

[SP 800-46] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2

[SP 800-50] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[SP 800-53] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP 800-53B] Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-53B. [Forthcoming].

[SP 800-56A] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[SP 800-57-1] Barker EB (2016) Recommendation for Key Management, Part 1: General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 4. https://doi.org/10.6028/NIST.SP.800-57pt1r4

[SP 800-58] Kuhn R, Walsh TJ, Fries S (2005) Security Considerations for Voice Over IP Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-58. https://doi.org/10.6028/NIST.SP.800-58

[SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of December 1, 2017. https://doi.org/10.6028/NIST.SP.800-63-3

[SP 800-70] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4

[SP 800-77] Frankel SE, Kent K, Lewkowski R, Orebaugh AD, Ritchey RW, Sharma SR (2005) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77. https://doi.org/10.6028/NIST.SP.800-77

[SP 800-83] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1

[SP 800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

[SP 800-86] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86

[SP 800-88] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[SP 800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[SP 800-94] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[SP 800-95] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95

[SP 800-97] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97

[SP 800-101] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1

[SP 800-111] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111

[SP 800-113] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[SP 800-114] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[SP 800-124] Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1. https://doi.org/10.6028/NIST.SP.800-124r1

[SP 800-125B] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B

[SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. https://doi.org/10.6028/NIST.SP.800-128

[SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[SP 800-160-1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-167] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167

[SP 800-171A] Ross RS, Dempsey KL, Pillitteri VY (2018) Assessing Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171A. https://doi.org/10.6028/NIST.SP.800-171A

[SP 800-181] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

MISCELLANEOUS PUBLICATIONS AND WEBSITES

[IETF 5905] Mills D, Martin J (ed.), Burbank J, Kasch W (2010) Network Time Protocol Version 4: Protocol and Algorithms Specification. (Internet Engineering Task Force), IETF Request for Comments (RFC) 5905. https://doi.org/10.17487/RFC5905

[NARA CUI] National Archives and Records Administration (2019) *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui

[NARA MARK] National Archives and Records Administration (2016) Marking Controlled Unclassified Information, Version 1.1. (National Archives, Washington, DC). https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

CUI Notice 2019-01, Controlled Unclassified Information Coversheets and Labels. https://www.archives.gov/files/cui/documents/20190222-cui-notice-2019-01-coversheet-label.pdf

[NIST CAVP] National Institute of Standards and Technology (2019) *Cryptographic Algorithm Validation Program*. https://csrc.nist.gov/projects/cavp

[NIST CMVP] National Institute of Standards and Technology (2019) *Cryptographic Module Validation Program*. https://csrc.nist.gov/projects/cmvp

[NIST CRYPTO] National Institute of Standards and Technology (2019) *Cryptographic Standards and Guidelines*. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST CUI] National Institute of Standards and Technology (2019) *Special Publication 800-171 Publication and Supporting Resources*. https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

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 [CNSSI 4009] *National Information Assurance Glossary*.

agency [OMB A-130]	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
assessment	See *security control assessment*.
assessor	See *security control assessor*.
audit log	A chronological record of system activities, including records of system accesses and operations performed in a given period.
audit record	An individual entry in an audit log related to an audited event.
authentication [FIPS 200, Adapted]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
availability [44 USC 3552]	Ensuring timely and reliable access to and use of information.
advanced persistent threat [SP 800-39]	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives.
baseline configuration	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

bidirectional authentication	Two parties authenticating each other at the same time. Also known as mutual authentication or two-way authentication.
blacklisting	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
confidentiality [44 USC 3552]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
configuration settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
controlled area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.
controlled unclassified information [EO 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 [32 CFR 2002]	Those types of information for which laws, regulations, or governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.
CUI Executive Agent [32 CFR 2002]	The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
CUI program [32 CFR 2002]	The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.

CUI registry [32 CFR 2002]	The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
cyber-physical systems	Interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.
dual authorization [CNSSI 4009, Adapted]	The system of storage and handling designed to prohibit individual access to certain resources by requiring the presence and actions of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.
executive agency [OMB A-130]	An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.
external system (or component)	A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
external system service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
external system service provider	A provider of external system services to an organization through a variety of consumer-producer relationships including, but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
external network	A network not controlled by the organization.
federal agency	See *executive agency*.
federal information system [40 USC 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. See *hardware* and *software*.
hardware [CNSSI 4009]	The material physical components of a system. See *software* and *firmware*.
identifier	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.
impact	With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.
impact value [FIPS 199]	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.
incident [44 USC 3552]	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
information [OMB A-130]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
information flow control	Procedure to ensure that information transfers within a system are not made in violation of the security policy.
information resources [44 USC 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.

information security [44 USC 3552]	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information system [44 USC 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
information technology [OMB A-130]	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
insider threat	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.
integrity [44 USC 3552]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
internal network	A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

least privilege	The principle that a security architecture is designed so that each entity is granted the minimum system authorizations and resources that the entity needs to perform its function.
local access	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.
mobile code	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.
mobile device	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.
multifactor authentication	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See *authenticator*.
mutual authentication [CNSSI 4009]	The process of both entities involved in a transaction verifying each other. See *bidirectional authentication*.
nonfederal organization	An entity that owns, operates, or maintains a nonfederal system.
nonfederal system	A system that does not meet the criteria for a federal system.
network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access	Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
nonlocal maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
on behalf of (an agency) [32 CFR 2002]	A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure.
personnel security [SP 800-53]	The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.
portable storage device	A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).
potential impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
privileged account	A system account with authorizations of a privileged user.
privileged user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
remote access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

remote maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
replay resistance	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
risk [OMB A-130]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
risk assessment [SP 800-30]	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
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 organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.
security assessment	See *security control assessment*.
security control [OMB A-130]	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
security control assessment [OMB A-130]	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 domain [CNSSI 4009, Adapted]	A domain that implements a security policy and is administered by a single authority.
security functions	The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

split tunneling	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.
system	See *information system*.
system component [SP 800-128]	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
system security plan	A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. In particular, the system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
system service	A capability provided by a system that facilitates information processing, storage, or transmission.
threat [SP 800-30]	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
system user	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
whitelisting	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.
wireless technology	Technology that permits the transfer of information between separated points without physical connection. Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
CISA	Cybersecurity and Infrastructure Security Agency
DMZ	Demilitarized Zone
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IoT	Internet of Things
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
IT	Information Technology
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
VoIP	Voice over Internet Protocol

APPENDIX D

MAPPING TABLES

MAPPING BASIC AND DERIVED SECURITY REQUIREMENTS TO SECURITY CONTROLS

Tables D-1 through D-14 provide a mapping of the basic and derived security requirements to the security controls in [SP 800-53].[31] The mapping tables are included for informational purposes and do not impart additional security requirements beyond those requirements defined in Chapter Three. In some cases, the security controls include additional expectations beyond those required to protect CUI and have been tailored using the criteria in Chapter Two. Only the portion of the security control relevant to the security requirement is applicable. The tables also include a secondary mapping of the security controls to the relevant controls in [ISO 27001]. An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control. Due to the tailoring actions carried out to develop the security requirements, satisfaction of a basic or derived requirement does *not* imply the corresponding NIST security control or control enhancement in [SP 800-53] has also been satisfied, 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 CSF] can use the mapping of the security requirements to the security controls in [SP 800-53] and [ISO 27001] to locate the equivalent controls in the Categories and Subcategories associated with the core Functions of the Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The control mapping information can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs, when such programs have been built around the NIST or ISO/IEC security controls.

[31] The security controls in Tables D-1 through D-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53B] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS

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

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

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

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

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

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

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

SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
	unauthorized access, modification, and deletion.			A.12.4.3	Administrator and operator logs
				A.18.1.3	Protection of records
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	AU-9(4)	Protection of Audit Information *Access by Subset of Privileged Users*	*No direct mapping.*	

TABLE D-4: MAPPING CONFIGURATION MANAGEMENT REQUIREMENTS TO CONTROLS[32]

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

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

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

TABLE D-5: MAPPING IDENTIFICATION AND AUTHENTICATION REQUIREMENTS TO CONTROLS[33]

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

[33] IA-2(8) is *not* currently in the NIST Special Publication 800-53 moderate security control baseline although it will be added to the baseline in the next update. Employing multifactor authentication without a replay-resistant capability for non-privileged accounts creates a significant vulnerability for systems transmitting CUI.

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

TABLE D-6: MAPPING INCIDENT RESPONSE REQUIREMENTS TO CONTROLS

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	IR-2	Incident Response Training	A.7.2.2*	
	IR-4	Incident Handling	A.16.1.4	
			A.16.1.5	
			A.16.1.6	
	IR-5	Incident Monitoring		
	IR-6	Incident Reporting	A.6.1.3	
			A.16.1.2	
	IR-7	Incident Response Assistance		
3.6.3 Test the organizational incident response capability.	IR-3	Incident Response Testing		

TABLE D-7: MAPPING MAINTENANCE REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.7 MAINTENANCE				
Basic Security Requirements				
3.7.1 Perform maintenance on organizational systems.	MA-2	Controlled Maintenance	A.11.2.4*	Equipment maintenance
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system 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 organizational systems.	MA-3(2)	Maintenance Tools *Inspect Media*	*No direct mapping.*	
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA-4	Nonlocal Maintenance	*No direct mapping.*	
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Maintenance Personnel	*No direct mapping.*	

TABLE D-8: MAPPING MEDIA PROTECTION REQUIREMENTS TO CONTROLS[34]

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8 MEDIA PROTECTION				
Basic Security Requirements				
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.	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 CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport *Cryptographic Protection*	*No direct mapping.*	
3.8.7 Control the use of removable media on system components.	MP-7	Media Use	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media

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

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

TABLE D-9: MAPPING PERSONNEL SECURITY REQUIREMENTS TO CONTROLS

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

TABLE D-10: MAPPING PHYSICAL PROTECTION REQUIREMENTS TO CONTROLS

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

TABLE D-11: MAPPING RISK ASSESSMENT REQUIREMENTS TO CONTROLS

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

TABLE D-12: MAPPING SECURITY ASSESSMENT REQUIREMENTS TO CONTROLS

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

TABLE D-13: MAPPING SYSTEM AND COMMUNICATIONS PROTECTION REQUIREMENTS TO CONTROLS[35]

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

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

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

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

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

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

APPENDIX E

TAILORING CRITERIA

LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53][36] moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.[37] 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;[38] or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.[39]

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

TABLE E: TAILORING ACTION SYMBOLS

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.

[36] The security controls in Tables E-1 through E-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53B] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

[37] The same *tailoring criteria* were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements described in Chapter Three.

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

[39] The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

TABLE E-1: TAILORING ACTIONS FOR ACCESS CONTROLS

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

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

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

TABLE E-3: TAILORING ACTIONS FOR 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 Logging Process Failures	CUI
AU-6	Audit Review, Analysis, and Reporting	CUI
AU-6(1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*	NCO
AU-6(3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*	CUI
AU-7	Audit Reduction and Report Generation	CUI
AU-7(1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*	NCO
AU-8	Time Stamps	CUI
AU-8(1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*	CUI
AU-9	Protection of Audit Information	CUI
AU-9(4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*	CUI
AU-11	Audit Record Retention	NCO
AU-12	Audit Generation	CUI

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

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

TABLE E-5: TAILORING ACTIONS FOR CONFIGURATION MANAGEMENT CONTROLS[40]

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

[40] 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[41]

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

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

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

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

TABLE E-8: TAILORING ACTIONS FOR INCIDENT RESPONSE CONTROLS

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

TABLE E-9: TAILORING ACTIONS FOR MAINTENANCE CONTROLS

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

TABLE E-10: TAILORING ACTIONS FOR MEDIA PROTECTION CONTROLS

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

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

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

TABLE E-12: TAILORING ACTIONS FOR PLANNING CONTROLS

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

TABLE E-13: TAILORING ACTIONS FOR PERSONNEL SECURITY CONTROLS

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

TABLE E-14: TAILORING ACTIONS FOR RISK ASSESSMENT CONTROLS

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

TABLE E-15: TAILORING ACTIONS FOR SYSTEM AND SERVICES ACQUISITION CONTROLS[42]

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

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

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

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

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

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