



National Institutes of Health
Turning Discovery Into Health

National Institutes of Health (NIH)
Office of the Director (OD)
Office of the Chief Information Officer (OCIO)
Information Security and Awareness Office (ISA0)

6555 Rock Spring Drive
Bethesda, MD 20817

NIH INFORMATION SECURITY (InfoSec)
POLICY HANDBOOK

VERSION 5.0
9 January 2019

FOR OFFICIAL USE ONLY

RECORD OF DOCUMENT CONTROL

This NIH Information Security (InfoSec) Policy Handbook may be updated as required to reflect regulatory, policy, standards, and organizational changes. Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed every three (3) years by the NIH Information Security and Awareness Office (NIH/OD/OCIO/ISAO) to ensure the Handbook remains relevant and accurate. Reviews and assessments made as part of this process are also included in the matrix below. This document history shall be maintained throughout the life cycle of this Handbook.

Version	Release Date	Summary of Changes	Section(s) Updated	Changes Approved By
1.0	05/27/2014	<ul style="list-style-type: none"> • Original Version. • Incorporated several parts of the previous NIH Enterprise Information System Security Plan (SSP) into the document. 	All	NIH/OD/OCIO/NIH InfoSec Program
2.0	04/29/2015	<ul style="list-style-type: none"> • Changed from a Guide to a Handbook. • Updated with policy statements and requirements that are necessary to satisfy a gap analysis of the HHS IS2P and NIST SP 800-53. • Added an appendix that provides more details control by control. • Added verbiage to state that NIH standards have equal bearing as policies. • Changed the purpose of the book from solely focusing on the Framework to also incorporating information that bridges the gaps between HHS policies, NIH policies, and the NIH IT Security Policy Framework. 	All	NIH/OD/OCIO/NIH InfoSec Program
3.0	04/01/2017	<ul style="list-style-type: none"> • Removed references to the NIH IT Security Policy Framework. • Updated the references throughout the document due to updates and rescinded policies. • Updated the roles and responsibilities to accurately reflect current operations. • Updated the waiver and IRT Portal access information. • Updated Appendix D to ensure all controls were addressed at the enterprise level, or by the IC. • Updated several sections in Appendix D to reflect current policies and operations. 	All	NIH/OD/OCIO/ISAO

Version	Release Date	Summary of Changes	Section(s) Updated	Changes Approved By
4.0	05/24/2018	<ul style="list-style-type: none"> • Reviewed and modified Handbook to be consistent with updated NIH policies. • Refined Handbook to include NIST SP 800-53, Rev 4 “<i>organization-defined</i>” values not defined in the HHS IS2P. • Refined Handbook to include HHS IS2P “<i>OpDiv-defined</i>” values. • Modified format to be more consistent with the HHS IS2P. • Added Program Management Controls. • Included edits and updates to Version 4.0 draft from NIH CISO, DCISO, and ISAO Managers and NIH OSOP reviews. 	All	NIH/OD/OCIO/ISAO
5.0	01/09/2019	<ul style="list-style-type: none"> • Reviewed document for accuracy, relevance, and effectiveness • Added policy note to the dash 1 control for each control family (AC-1, AT-1, AU-1, etc.). • Changed font color for Notes in controls to Green. • Updated content for the following Security controls in Appendix B: AC-2(4), AC-19(5), AC-21, AU-3(2), AU-5, AU-5 (c.e.2), CA-2, CA-7, CM-3, CM-5 (c.e.2), CM-7 (c.e.5), CP-8 (c.e.4), IA-2 (c.e.11), IA-5, MA-4 (c.e.1), MP-6, PL-4, PM-1, PM-9, PS-7, RA-3, SC-7(8), SI-2 • Added notes to AC-7 and IA-5 c.e.1 to comply with HHS IS2P Addendum • Updated AC-18 c.e.1, c.e.4, and c.e.5 for all baselines to comply with HHS IS2P Addendum • Added AC-18 c.e.3 for all baselines to comply with HHS IS2P Addendum • Incorporated Program Management Controls into Security Controls • Added Appendix D, Acronym List • Expanded and updated the Glossary (Appendix E) 	All	NIH/OD/OCIO/ISAO

RECORD OF DOCUMENT APPROVAL

This signature page serves as the official record of approval for the NIH Information Security (InfoSec) Policy Handbook. The effective date of this Handbook is the signature date.

NIH Authorizing Official Signature:

Christopher S. Todd
NIH Chief Information Security Officer (CISO)

TABLE OF CONTENTS

1	Introduction.....	8
1.1	Purpose.....	8
1.2	Background.....	9
1.3	Scope.....	9
1.4	Coordination Among Organizational Entities	10
1.4.1	HHS-Level Coordination.....	10
1.4.2	NIH-Level Coordination.....	10
1.4.3	IC-Level Coordination.....	10
1.5	Authorities.....	10
1.6	References and Attribution	11
1.7	Document Approval Date	13
1.8	Document Effective Date.....	13
1.9	Document Review.....	14
1.10	Assistance	14
2	Policy	15
2.1	HHS-Mandated Controls	15
2.1.1	Methodology for Assessment and Authorization (A&A).....	15
2.1.2	Risk-Based Protection.....	15
2.1.3	HHS Security and Privacy Control Assignments and Selections	15
2.1.3.1	Deviations from HHS Assignments and Selections.....	15
2.1.3.2	Exercising Flexibility.....	15
2.1.4	Conducting Information Security and Privacy Activities.....	16
2.1.5	Adherence to Newly Published Federal Requirements	16
2.1.5.1	New Federal Requirement Cannot be Implemented (Development System). 16	
2.1.5.2	New Federal Requirement Cannot be Implemented (Operational System).... 16	
2.1.6	Employing Compensating Security Controls.....	17
2.1.7	Applying the HHS IS2P.....	17
2.2	NIH Controls.....	17
2.2.1	NIH-Wide Security Controls	17
2.2.2	System-Specific Security Controls	17
3	Appendix A: Roles and Responsibilities	18
3.1	NIH Enterprise-Level Roles and Responsibilities	18
3.1.1	NIH Office of the Director (NIH OD)	18
3.1.2	NIH Chief Information Officer (CIO)	19
3.1.3	NIH Chief Information Security Officer (CISO).....	20
3.1.4	NIH Threat Mitigation & Incident Response (TMIR).....	22
3.1.5	NIH Senior Official for Privacy (SOP).....	22
3.1.6	NIH Authorizing Official (AO) or AO Designated Representative	24
3.2	NIH Office-Level and Institutes and Centers (ICs) Roles and Responsibilities.....	25
3.2.1	Chief Information Officer (CIO)	25
3.2.2	Chief Information Security Officer (CISO).....	26
3.2.3	Information System Security Officers (ISSO).....	27

3.2.4 Privacy Coordinator 29

3.2.5 Security Control Assessor..... 30

3.2.6 Program Executive..... 31

3.2.7 System Owner..... 31

3.2.8 Data Owner/Business Owner..... 35

3.2.9 Website Owner/Administrator 35

3.2.10 Project/Program Manager 35

3.2.11 Contingency Planning Coordinator..... 36

3.2.12 System Developer and Maintainer..... 36

3.2.13 System/Network Administrator 37

3.2.14 Contracting Officer (CO) and Contracting Officer’s Representative (COR) 39

3.2.15 Supervisor 40

3.2.16 All Users 40

4 Appendix B: Security Controls Section..... 42

4.1 Access Control (AC)..... 43

4.2 Awareness and Training (AT) 61

4.3 Audit and Accountability (AU) 64

4.4 System Assessment and Authorization (CA)..... 75

4.5 Configuration Management (CM) 85

4.6 Contingency Planning (CP) 98

4.7 Identification and Authentication (IA)..... 107

4.8 Incident Response (IR) 116

4.9 Maintenance (MA)..... 120

4.10 Media Protection (MP) 126

4.11 Physical and Environmental Protection (PE)..... 129

4.12 Planning (PL) 135

4.13 Program Management (PM) 140

4.14 Personnel Security (PS) 146

4.15 Risk Assessment (RA)..... 153

4.16 Systems and Services Acquisition (SA) 157

4.17 Security and Communications Protection (SC)..... 165

4.18 System and Information Integrity (SI)..... 172

5 Appendix C: Privacy Controls Section..... 180

5.1 Authority and Purpose (AP)..... 181

5.2 Accountability, Audit, and Risk Management (AR) 182

5.3 Data Quality and Integrity (DI)..... 186

5.4 Data Minimization and Retention (DM)..... 187

5.5 Individual Participation and Redress (IP) 189

5.6 Security (SE)..... 191

5.7 Transparency (TR)..... 193

5.8 Use Limitation (UL) 196

6 Appendix D: Acronyms List..... 197

7 Appendix E: Glossary 207

8 Appendix F: Minimum Set of HHS and NIH Roles Assigned Significant Responsibilities for Information Security 254

9 Appendix G: System Component Inventory Requirements..... 257
10 Appendix H: Information System Media..... 258

1 Introduction

1.1 Purpose

The National Institutes of Health (NIH), Office of the Director (OD), Office of the Chief Information Officer (OCIO), Information Security and Awareness Office (ISAO), *NIH Information Security (InfoSec) Policy Handbook* (henceforth the “Handbook”) provides direction to NIH and the Institutes and Centers (ICs) information technology (IT) security programs for the security and privacy of NIH data in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).¹

The Handbook supplements The Department of Health and Human Services (HHS), Office of the Chief Information Officer (OCIO), *HHS-OCIO Information Systems Security and Privacy Policy* (henceforth “the IS2P”), which provides direction to the IT security programs of Operating Divisions (OpDivs) and Staff Divisions (StaffDivs) for the security and privacy of HHS data. Specifically, the Handbook defines security and privacy control requirements and guidance where the HHS IS2P delegates the definition of the security and privacy control requirements and guidance to NIH.

The Handbook is a reissuance in order to comply with the updated requirements of the *National Institute of Standards and Technology’s (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*, (henceforth “NIST SP 800-53, Rev 4”) as amended. This Policy establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of NIH and the ICs. For the controls that are to be applied without needing any specific IC parameters, this Policy will be the authoritative source. ICs do not have to develop internal policies to supplement the stated requirements. The Handbook also includes the complementary [Security Controls Section](#) and [Privacy Controls Section](#). These sections outline IT security, privacy and program management policy requirements for IT security and privacy programs and information systems in more detail and is organized according to information assurance (IA) control families (as defined by NIST SP 800-53, Rev 4) to make the document easy to use and scalable for the future.

This Handbook supersedes previous versions of this document. This document does not supersede any other applicable law or higher-level HHS policies, directives, memorandum, or standards. All references noted this Handbook are subject to periodic revision, update, and reissuance.

The Handbook codifies NIH’s authority to develop, document, implement, and oversee an NIH enterprise-wide IT security and privacy program to provide IT security and privacy for the information and information systems that support the operations and assets of NIH, including those provided or managed by another Federal agency, contractor, or other source. ICs must comply with and support the implementation of HHS- and NIH-wide IT security and privacy programs, to include compliance with Federal requirements and programmatic policies, standards, procedures, and IT security controls.

¹ Formerly the Federal Information Security Management Act of 2002 (FISMA).

1.2 Background

The NIH Information Security (InfoSec) Program (henceforth the “NIH InfoSec Program”), which is managed and operated by the NIH ISAO, has evolved and matured over the last several years as new Federal requirements have been published, as advances in technology have been made, and as new threats to NIH’s infrastructure have emerged. Additionally, concerns over the unauthorized disclosure of protected health information (PHI) and personally identifiable information (PII) have placed IT security and privacy issues at the forefront of the national dialogue, positively impacting the way in which public, private, and government organizations provide services and protect information.

To better serve IT security and privacy stakeholders, HHS and NIH recognized the need to appropriately incorporate, cross-reference, and organize its IT security and privacy policy requirements in a manner that clearly explains the scope and applicability of the requirements. The format in which those requirements are presented should be scalable to accommodate the modification or addition of new requirements over time. As a result, this Handbook was developed to incorporate privacy requirements as well as other requirements cross-referenced in individually-released NIH policies, standards, and memoranda.

1.3 Scope

This Handbook applies to all ICs, and all personnel conducting business for, and on behalf of, NIH, whether directly or through contractual relationships. This Handbook does not supersede any other applicable law, higher level HHS or NIH directives, or existing labor management agreements in place as of the effective date of this Handbook.

NIH officials must apply this Handbook to employees, contractor personnel, interns, fellows, guests, and other non-government employees conducting business for the NIH, or on its behalf through contractual relationships or memoranda of agreement, when using HHS or NIH information systems or resources. All organizations collecting or maintaining information or using or operating information systems on behalf of the NIH, are also subject to the stipulations of this Handbook. The content of and compliance with this Handbook must be incorporated into applicable contract language, as appropriate.

ICs shall use this Handbook or may create more restrictive IC security and privacy controls directives, policies, and guidance to meet the specific needs of the IC’s mission objectives and information security requirements. The resulting IC directive, policy, or guidance shall be in no way less restrictive, less comprehensive, or less compliant with this Handbook.

NIH acknowledges that ICs require flexibility in implementing this Handbook. Variations in terminology may currently exist across NIH and the ICs, and there may be variations in the titles of roles. These variations are acceptable. For cases in which an IC cannot comply with these requirements, justification for noncompliance must be documented using the *NIH Information Security Policy/Standard Waiver*.²

² Justification may also be documented in security artifacts, such as System Security Plans (SSP) drafted pursuant to the NIST SP 800-37, which are subject to approval by the NIH Authorizing Official (AO).

1.4 Coordination Among Organizational Entities

1.4.1 HHS-Level Coordination

NIH ISAO refers to HHS Cybersecurity Program and HHS Privacy Program policies, standards, memoranda, guides, and standard operating procedures to ensure the Handbook complies with HHS mandates. This includes coordinating with the HHS OCIO, HHS Chief Information Security Officer (CISO), HHS Office of the Chief Privacy Officer, and Privacy Resource Center to clarify HHS mandated information and seek guidance on security and privacy controls issues as needed.

1.4.2 NIH-Level Coordination

NIH ISAO coordinates with the NIH OCIO and NIH Senior Official for Privacy (SOP) to ensure NIH InfoSec Program policies, standards, memoranda, guides, and standard operating procedures, to include this Handbook, are representative of NIH's information security and privacy requirements.

1.4.3 IC-Level Coordination

The NIH ISAO coordinates with the IC CISOs and ISSOs on NIH InfoSec Program policies, standards, memoranda, guides, and standard operating procedures, to include this Handbook, to ensure the NIH InfoSec Program and Handbook provides the requisite direction and guidance for the IC CISOs and ISSOs to operate and manage the IC InfoSec Programs. The IC CISOs and ISSOs are the principal contacts for coordination, implementation, communication, and application of IT security policies in conjunction with the NIH CISO.

The NIH Information Technology Management Council Security and Privacy Subcommittee (ITMC-SPS) Meeting is also an important coordination mechanism for the NIH ISAO and NIH CISO to collaborate with the ICs on NIH InfoSec Program activities. The ITMC-SPS provides leadership and direction on the NIH-wide IT security initiative to modify all computers, applications, and network components as necessary to mitigate risks and address problems and threats to information security and privacy.

In addition, the NIH ISAO provides IC Information Security Reports, at least quarterly, to the IC senior leadership to include the CIO, CISO, and ISSO. These reports provide an assessment the IC's information security risk posture and a consolidated view of the current NIH information security priorities.

1.5 Authorities

The Office of Management and Budget (OMB) Circular A-130, Appendix III, and the Federal Information Security Modernization Act (FISMA), require federal agencies to protect their information resources and data by establishing information security programs and imposing special requirements for protecting sensitive data and Personally Identifiable Information (PII). This Handbook codifies NIH's authority to develop, document, implement, and oversee an NIH enterprise-wide IT security and privacy program.

1.6 References and Attribution

The following laws, regulations, policies, standards, and guidelines were used to provide the content for and compile this Handbook:

- 5 United States Code (U.S.C.) § 552a, Privacy Act of 1974
- 20 U.S.C, Chapter 31, Part 4, Section (Sec.) 123g, Family Educational and Privacy Rights
- 44 U.S.C., Chapter 36, Public Printing and Documents, Management and Promotion of Electronic Government Services (also known as E-Government Act of 2002)
- 44 U.S.C., Sec. 3502, Public Printing and Documents, Coordination of Federal Information Policy, Federal Information Policy
- 44 U.S.C., Sec. 3544, Public Printing and Documents, Coordination of Federal Information Policy, Information Security
- Chief Information Officers Council Federal Enterprise Architecture Framework Version 1.1
- Committee on National Security Systems Instruction (CNSSI) 4009, National Information Assurance (IA) Glossary
- Common Approach to Federal Enterprise Architecture
- Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. (Defined in the HIPAA Privacy Rule)
- Federal Information Security Modernization Act of 2014 (FISMA)
- FIPS 140-2, Security Requirements for Cryptographic Modules
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 201-1, Personal Identity Verification for Federal Employees and Contractors
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- HHS Information Security and Privacy Policy (IS2P)
- Addendum to the HHS Information Security and Privacy Policy (IS2P)
- HHS Office of Information Security High Value Asset Program Policy
- HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- HHS Policy for Enterprise Architecture
- HHS Policy for Enterprise Performance Life Cycle (EPLC)
- HHS Policy for Information Technology
- HHS Policy for Information Technology (IT) Policy Development
- HHS Policy for IT Security and Privacy Incident Reporting and Response
- HHS Rules of Behavior for Use of HHS Information and IT Resources Policy
- HHS Standard for Encryption of Computing Devices and Information
- HHS Standard for Plans of Action and Milestones Management and Reporting
- Homeland Security Presidential Directive 12 (HSPD-12)
- Institute of Electrical and Electronic Engineers (IEEE) 610.12, Standard Glossary of Software Engineering Terminology

- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003
- International Association of Privacy Professionals Site Glossary
- NIH Information Technology General Rules of Behavior
- NIH Information Security Incident Response Plan
- NIH Mobile Device Security Policy
- NIH Mobile Device Security Standard
- NIH Policy Manual Chapters:
 - 1405 - NIH Physical Access Control
 - 1440 - Dissemination of Security and Intelligence-Related Information
 - 1745 - NIH Information Technology (IT) Privacy Program
 - 1745-1 - NIH Privacy Impact Assessments
 - 1745-2 - NIH Privacy and Information Security Incident and Breach Response Policy
 - 1750 - NIH Risk Management Program
 - 1825 - Information Collection from The Public
 - 2801 - Access Control Facilities on Mainframe Computers
 - 2804 - Public-facing Web Management Policy
 - 2805 - NIH Web Privacy Policy
 - 2810 - NIH Remote Access Policy
 - 2811 - NIH Policy on Smart Card Authentication
 - 2813 - NIH Information Security and Privacy Awareness Training Policy
 - 2814 - NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment
 - 2815 - NIH Policy on the Use of Peer-to-Peer Software
 - 2817 - NIH Policy for Special Computer Monitoring of Employee Use of Information Technology (IT)
- NIH Wireless Network Security Policy
- NIH Wireless Network Security Standard
- NIST SP 800-12, An Introduction to Information Security
- NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST SP 800-18, Guide for Developing System Security Plan (SSP)s for Federal Information Systems
- NIST SP 800-27A, Engineering Principles for Information Technology Security [A Baseline for Achieving Security]
- NIST SP 800-28 Version 2, Guidelines on Active Content and Mobile Code
- NIST SP 800-28, Guidelines on Active Content and Mobile Code
- NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program
- NIST SP 800-46, Security for Telecommuting and Broadband Communications

- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
- NIST SP 800-55, Performance Measurement Guide for Information Security
- NIST SP 800-57, Recommendation for Key Management
- NIST SP 800-58, Security Considerations for Voice Over IP Systems)
- NIST SP 800-59, Guideline for Identifying an Information System as a National Security System
- NIST SP 800-61, Computer Security Incident Handling Guide
- NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide
- NIST SP 800-88, Guidelines for Media Sanitization
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- Office of Personnel Management (OPM) Regulation 5 Code of Federal Regulations (CFR) 930.301
- Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, Revised July 2016
- OMB M-02-01, Guidance for Preparing and Submitting System Security Plan (SSP)s of Action and Milestones
- OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB M-04-26, Personal Use Policies and ‘File Sharing’ Technologies
- OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies
- OMB M-10-23 Guidance for Agency Use of Third-Party Websites and Applications
- OMB M-17-12 Preparing for and Responding to a Breach of Personally Identifiable Information
- The Information Security Automation Program and The Security Content Automation Protocol as released by the NIST National Vulnerability Database
- United States Computer Emergency Readiness Team (US-CERT) Quarterly Trends and Analysis Report, Volume 1, Issue 2

1.7 Document Approval Date

The Handbook approval date is the Authorizing Official signature date, which is located on the Record of Document Approval page.

1.8 Document Effective Date

The Handbook effective date is six (6) months after the approval date. All NIH ICs and Offices must implement the policies and requirements in this Handbook no later than six (6) months after the Handbook is approved.

1.9 Document Review

At a minimum, this document will be reviewed and assessed every three (3) years by the NIH Information Security and Awareness Office (NIH/OD/OCIO/ISAO) to ensure the Handbook remains relevant and accurate. The details associated with these reviews and updates are captured on the Version History page.

1.10 Assistance

For more information on the NIH InfoSec Program, please visit <https://ocio.nih.gov/InfoSecurity/Pages/default.aspx>

Please direct any questions, comments, suggestions, or requests for further information to the NIH InfoSec Program at NIHInfoSec@nih.gov or 301-881-9726.

2 Policy

2.1 HHS-Mandated Controls

This section addresses HHS mandates for the secure development, operations, and maintenance of information systems.

2.1.1 *Methodology for Assessment and Authorization (A&A)*

NIH must use *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, as the methodology for assessment and authorization (A&A)³ of information systems, in accordance with FISMA and direction from the Office of Management and Budget (OMB).

2.1.2 *Risk-Based Protection*

NIH must ensure that information systems provide adequate, risk-based protection in the control areas defined in the *Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems*, by using the appropriate baseline security controls as established in *NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations* in accordance with the impact level for the system as defined in *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*.

2.1.3 *HHS Security and Privacy Control Assignments and Selections*

For instances in which NIST directs agencies to make assignments and selections within the confines of NIST SP 800-53, Rev 4 controls, the HHS IS2P provides the standard parameters which NIH must utilize for systems categorized as Low, Moderate, or High. The term “the organization” is used throughout these controls to make clear that, unless a component is specifically mentioned, these are a baseline regardless of organizational component or system and may be enhanced as necessary based on that component’s mission.

2.1.3.1 *Deviations from HHS Assignments and Selections*

Deviations from the HHS assignments and selections within the [Security Controls Section \(Appendix B\)](#) are permitted, providing the resulting parameters are consistent with NIST SP 800-53, Rev 4 or minimum government-wide parameters. Exceptions cannot be granted to the controls themselves as they are Federal Government-wide standards; however, the compensating security control policy applies (See [Section 2.1.6, Employing Compensating Security Controls](#).)

2.1.3.2 *Exercising Flexibility*

NIH may exercise flexibility in the solutions used to meet the control requirement, so long as the baseline requirement is met.

³ At NIH, Assessment and Authorization (A&A) was formerly known as Certification and Accreditation (C&A) and more recently formerly known as Security Assessment and Authorization (SA&A). Some documents and processes may still contain and use the older terminologies. Since some ICs are using the term SA&A, A&A and SA&A are used interchangeably at NIH.

2.1.4 Conducting Information Security and Privacy Activities

Information security and privacy activities conducted within HHS must be consistent with the guidance, methodologies, and intent prescribed by the NIST SP series, NIST SP 800-53, Rev 4, and other relevant Federal laws and guidance documents. It is incumbent upon NIH to appropriately follow the steps in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* to select, implement, assess, authorize, and monitor such controls commensurate with a system's FIPS 199 categorization.

2.1.5 Adherence to Newly Published Federal Requirements

In accordance with the HHS IS2P, Section 4 (Policy) and the HHS Plan of Action and Milestones Standard, as new Federal requirements are published, NIH must ensure that systems that are in development comply with those newly published requirements before those systems are granted a security authorization, and that existing (i.e., operational) systems comply with the new requirements within one year.

2.1.5.1 New Federal Requirement Cannot be Implemented (Development System)

If any issues are identified that would prevent the implementation of a new Federal requirement on a development system, the Information System Security Officer (ISSO) or System Owner must bring this issue to the attention of the Authorizing Official (AO) or the AO Designated Representative as soon as the issue is identified so that a plan can be developed to implement or mitigate the requirement, or the risk can be accepted. When the final security authorization package is delivered, and it has been agreed that the requirement would not be implemented, the AO or AO Designated Representative must acknowledge the gap in the form of a Plan of Action and Milestones (POA&M), and must indicate an anticipated time period when the requirement will be met or explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

2.1.5.2 New Federal Requirement Cannot be Implemented (Operational System)

If a new Federal requirement cannot be implemented on an operational system, the ISSO or System Owner must bring this to the attention of the AO or AO Designated Representative. The AO or AO Designated Representative must acknowledge the gap in the form of a Plan of Action and Milestones (POA&M) and must either indicate an anticipated time period when the requirement will be met or document the risk-based decision not to comply with the requirement.

2.1.6 *Employing Compensating Security Controls*

NIH (including the ICs) may employ compensating security controls only after the following conditions are met:

1. NIH selects the compensating security control(s) from the security control catalog in NIST SP 800-53, Rev 4, when applicable;
2. NIH develops a complete and convincing rationale and justification for how the chosen compensating security control(s) provide an equivalent security capability or level of protection for the information system;
3. NIH assesses and formally accepts (i.e., in writing) the risk associated with employing the compensating security control(s) in the information system; and
4. NIH must review the use of compensating security controls, document those controls in the System Security Plan (SSP) and other appropriate security documentation for the information system, and request approval of those controls from the AO or AO Designated Representative for the information system.

2.1.7 *Applying the HHS IS2P*

NIH must apply the controls in HHS IS2P to its IT security and privacy program and to its information systems, as appropriate. HHS updated the IS2P and accompanying *HHS Office of the Secretary Procedures Handbook for Information Security* by integrating and establishing the HHS minimum requirements for IT security and privacy programs with NIH and to address common system security control questions that fall outside the scope of NIST SP 800-53, Rev 4.

2.2 NIH Controls

This section establishes the authority for NIH to develop its own NIH-wide security and privacy controls for information systems and codify the controls in this Handbook.

2.2.1 *NIH-Wide Security Controls*

In accordance with the HHS IS2P, NIH may decide whether to issue any additional NIH-wide security and privacy controls for NIH and IC information systems to augment the Government and HHS-wide controls. NIH must ensure that parameters are established and documented for organization- and OpDiv-defined control, unless set by HHS.

2.2.2 *System-Specific Security Controls*

In accordance with the HHS IS2P, NIH may develop system-specific security and privacy controls and parameters. When needed and/or appropriate, it is an NIH decision whether to set parameters NIH-wide, on a system-by-system basis, or some combination thereof.

3 Appendix A: Roles and Responsibilities

3.1 NIH Enterprise-Level Roles and Responsibilities

3.1.1 NIH Office of the Director (NIH OD)

The responsibilities of the NIH OD include, but are not limited to:

- Providing IT security and privacy protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the following:
 - Information collected or maintained by or on behalf of NIH; and
 - Information systems used or operated by NIH, a contractor of the NIH, or another organization on behalf of the NIH.
- Complying with the requirements of FISMA (Title III of the E-Government Act) and HHS-related policies, procedures, standards, and guidelines, including:
 - IT security and privacy requirements promulgated under OMB Circular A-130, Appendix III; and
 - IT security and privacy standards and guidelines issued by OMB in accordance with NIST guidance, including Presidential Directives such as Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standards for Federal Employees and Contractors.
- Ensuring that IT security and privacy management processes are integrated with NIH strategic and operational planning processes.
- Ensuring that senior NIH officials provide IT security and privacy for the information and information systems that support the operations and assets under their control.
- Designating a senior NIH official as the NIH CIO and delegating to the NIH CIO the authority to ensure compliance with the security requirements imposed on the NIH under FISMA.
- Delegating responsibility and authority for management of NIH IT security and privacy programs to the NIH CIO.
- Ensuring that NIH has trained personnel sufficiently to assist NIH in complying with the security and privacy requirements under FISMA and HHS policies.
- Ensuring that the NIH CIO, in coordination with other senior NIH officials, reports annually to NIH OD on the effectiveness of the NIH InfoSec Program, including the progress of any remedial actions.

3.1.2 *NIH Chief Information Officer (CIO)*

The responsibilities of the NIH CIO⁴ are to provide leadership to activities including, but not limited to:

- Reporting annually to NIH OD on the effectiveness of the NIH InfoSec Program, including the progress of any remedial actions.
- Reporting quarterly to the HHS CIO on the effectiveness of the NIH InfoSec Program, including the progress of any remedial actions.
- Appointing an NIH CISO to fulfill the responsibilities of the NIH CIO in maintaining the NIH InfoSec Program.
- Managing NIH internal security reviews of the program business cases, alternatives analyses, and other specific investment documents.
- Managing and certifying an inventory of all current and proposed investments containing an IT component in accordance with the HHS Capital Planning and Investment Control (CPIC) process.
- Ensuring that policies, procedures, and practices are consistent with HHS requirements in order to ensure that programs, systems, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources, unintended release of HHS and NIH data, or denial of service (DoS).
- Ensuring that all employees and contractors comply with HHS Cybersecurity Program and NIH InfoSec Program security and privacy policies.
- Ensuring the establishment of a computer security incident response team (CSIRT)⁵ to participate in the investigation and resolution of incidents within NIH.
- Establishing, implementing, and enforcing an NIH-wide framework to facilitate an incident response program (including PII and PHI breaches) that ensures proper and timely reporting to HHS.
- Managing an inventory of all major information systems, devices and other items per FISMA requirements and as required by OMB.
- Ensuring mandatory security training, education, and awareness activities are undertaken by all personnel using, operating, supervising, or managing information systems.
- Exercising primary responsibility and authority for management of the NIH InfoSec Program.

⁴ The NIH CIO performs the NIH Risk Executive function on behalf of the NIH OD.

⁵ At NIH, the CSIRT or NIH Incident Response Team (IRT) is known as Threat Mitigation & Incident Response (TMIR). CSIRT and NIH IRT at the NIH-level is referred to as TMIR throughout this document.

- Serves as one of six HHS Primary Operational IT Infrastructure Managers⁶.
- Resolving any disputes from Office of the Inspector General (OIG) reviews and audits at the NIH level, where possible. If disputes cannot be resolved, the disputes must be escalated to the HHS CIO.
- Developing a strategy for the continuous monitoring⁷ of security control effectiveness and any proposed or actual changes to the information system and its environment of operation⁸.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.1.3 NIH Chief Information Security Officer (CISO)

The responsibilities of the NIH CISO include, but are not limited to:

- Leading the NIH InfoSec Program and promoting proper IT security and privacy practices.
- Supporting the HHS CISO in the implementation of the HHS Cybersecurity Program.
- Fostering communication and collaboration among the NIH security and privacy stakeholders to share knowledge and to better understand threats to NIH information.
- Providing information about the NIH InfoSec Program IT security and privacy policies to management and throughout NIH.
- Providing advice and assistance to other organizational personnel concerning the security of sensitive information and of critical data processing capabilities.
- Advising the NIH CIO about security-related incidents in accordance with the security breach reporting procedures developed and implemented by HHS and NIH.
- Disseminating information on potential security threats and recommended safeguards.

⁶ Applies to the CIO for the Centers for Disease Control and Prevention (CDC), Food and Drug Administration (FDA), Indian Health Service (IHS), Centers for Medicare and Medicaid Services (CMS), **National Institutes of Health (NIH)**, and Office of the Secretary (OS). When an OpDiv CIO performs as a Primary Operational IT Infrastructure Manager, he/she is responsible for performing IT risk-management duties. Where an information system relies (or partially relies) on one of the six Primary Operational IT infrastructures, the associated Primary Operational IT Infrastructure Manager(s) must concur with the risk acceptance by also signing the security authorization package as the AO.

⁷ The monitoring strategy may be included in the System Security Plan (SSP) to support the concept of near real-time risk management and ongoing authorization. The approval of the monitoring strategy may be obtained in conjunction with the SSP approval. The monitoring of security controls continues throughout the Enterprise Performance Life Cycle (EPLC).

⁸ This is the responsibility of the System Owner or the Primary Operational IT Infrastructure Manager.

- Ensuring NIH-wide implementation of HHS and NIH policies and procedures that relate to IT security and privacy incident response and executing the responsibilities detailed in *NIH Policy Manual Chapter 1745-2, NIH Privacy and Information Security Incident and Breach Response Policy*.
- Collaborating with the HHS Privacy Incident Response Team (HHS PIRT) Coordinator when the HHS PIRT Coordinator is engaging NIH TMIR for information collection and clarification and sitting on the HHS PIRT while the breach is under investigation.
- Coordinating with NIH Senior Official for Privacy (SOP) to ensure privacy implications are addressed when PII incident response activities occur within NIH.
- Ensuring that roles with significant security responsibilities are identified and documented per the HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities.
- Conducting security education and awareness training needs assessments to determine appropriate training resources and to coordinate training activities for target populations.
- Supporting general privacy awareness and RBT activities for all personnel using, operating, supervising, or managing information systems.
- Assisting System Owners in establishing and implementing the required security safeguards to protect computer hardware, software, and data from improper use or abuse.
- Coordinating requirements for personnel clearances, position sensitivity, and access to information systems with the appropriate office.
- Establishing, documenting, and enforcing requirements and processes for granting and terminating all administrative privileges including, but not limited to, servers, security domains, and local workstations.
- Reviewing contracts, with assistance from IC CISOs and/or ISSOs, for systems under the NIH CISO's control to ensure that IT security is appropriately addressed in contract language.
- Auditing the processes above for effectiveness.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.1.4 NIH Threat Mitigation & Incident Response (TMIR)⁹

The responsibilities of the NIH TMIR include, but are not limited to:

- Serves as the primary entity in NIH responsible for maintaining NIH-wide operational IT security situational awareness and determining the overall IT security risk posture of NIH.
- Serves as the lead organization for coordinating NIH-wide cybersecurity information sharing, analysis, and response activities.
- Reports NIH IT security and privacy incidents to HHS Computer Security Incident Response Center (CSIRC).
- Serves as NIH's primary POC with HHS CSIRC.

3.1.5 NIH Senior Official for Privacy (SOP)

The responsibilities of NIH SOP include, but are not limited to:

- Supporting the HHS Senior Agency Official for Privacy (SAOP) in ad-hoc privacy reporting activities as necessary, including the maintenance of and compliance with Presidential mandates and quarterly and annual FISMA reporting activities.
- Reviewing and approving NIH FISMA and Privacy Management Report for submission to HHS.
- Developing and supporting the integration of the HHS privacy program initiatives into IT security practices, where applicable.
- Establishing and implementing privacy policies, procedures, and practices consistent with HHS privacy requirements, in coordination with the NIH CISO.
- Coordinating NIH policy, guidance, and system-level documentation to ensure that HHS management, operational, and technical privacy requirements are addressed.
- Approving written requests to process, access, or store PII on personally owned or non-HHS or non-NIH equipment in accordance with the Security Controls Section AC-17: Remote Access.
- Coordinating with the NIH CISO to obtain contractual assurances from third parties to ensure that the third party will protect PII in a manner consistent with the privacy practices of HHS and NIH.

⁹ At NIH, the Incident Response Team (IRT) is Threat Mitigation & Incident Response (TMIR). TMIR managed by the NIH CISO and a part of NIH/OD/OCIO/ISAO. For this reason, IRT at the NIH-level is referred to as TMIR throughout this document.

- Reporting, in coordination with the NIH CISO, to the HHS SAOP the effectiveness of the NIH privacy program, including weaknesses and the progress of remedial actions, as identified.
- Establishing an NIH policy framework to facilitate the development and maintenance of Privacy Impact Assessments (PIAs) for all systems based on HHS and Federal legislative requirements.
- Tracking and maintaining all NIH PIA activities in the HHS PIA reporting tool.
- Reviewing completed NIH PIAs and attesting that PIAs are adequately and accurately completed.
- Promoting (i.e., escalating) NIH PIAs to HHS, and submitting completed NIH PIAs to the HHS SAOP, and/or seeking revisions from the PIA author if errors are found.
- Coordinating activities to regularly review PII holdings, assessing the PII confidentiality impact level of the PII holdings, recommending controls to protect the confidentiality of the PII, and eliminating the unnecessary use or collection of PII (including social security numbers).
- Coordinating and ensuring that privacy education and awareness activities, specific to the NIH privacy culture, are established for all personnel using, operating, supervising, or managing information systems.
- Coordinating with the NIH budgetary offices to ensure PIA and System of Records Notice (SORN) activities are included as part of Exhibit 300 development.
- Making recommendations to the HHS SAOP and senior level officials with budgetary authority in order to allocate proper resources to identify and mitigate privacy weaknesses found in system PIAs.
- Coordinating reviews of data sharing activities to ensure that reviews occur according to applicable privacy laws and with appropriate safeguards.
- Coordinating with HHS Website owners/administrators to ensure that Web-based privacy compliance requirements are met across the NIH.
- Coordinating with the NIH Threat Mitigation & Incident Response (TMIR) and/or HHS PIRT concerning reports of the loss of control of PII and executing the responsibilities detailed in *NIH Policy Manual Chapter 1745-2, NIH Privacy and Information Security Incident and Breach Response Policy*.

3.1.6 *NIH Authorizing Official (AO) or AO Designated Representative*

The responsibilities of the AO or AO Designated Representative¹⁰ for systems and networks under his or her authority include, but are not limited to, the following:

- In collaboration with the NIH CISO, determining through the security authorization process whether to accept residual risks or to implement appropriate risk mitigation countermeasures, based on the analysis provided by the Security Control Assessor (or designee).
- Making the final system security authorization decision and signing the authorization decision document.
- Ensuring that sensitive information is protected from unauthorized access in all forms at rest or in transit.
- Maintaining budgetary oversight for an information system or responsibility for the mission and/or business operations supported by the system.
- Maintaining accountability, through the security authorization process, for the security risks associated with information system operations.
- Providing written authorization accepting responsibility and risk for operating a system or application not in compliance with the HHS minimum standard.
- Determining (with the NIH CIO), based on organizational priorities, the appropriate allocation of resources dedicated to the protection of the information systems supporting the organization's missions and business functions.
- Approving the continuous monitoring strategy including the set of security controls that are to be monitored on an ongoing basis and the frequency of the monitoring activities.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

¹⁰ At NIH, the NIH CIO designated the NIH CISO as the Authorizing Official (AO) for all Authorizations to Operate (ATOs) for NIH and ICs information systems.

3.2 NIH Office-Level and Institutes and Centers (ICs) Roles and Responsibilities

3.2.1 Chief Information Officer (CIO)

The responsibilities of the CIO are to provide leadership to activities including, but not limited to:

- Reporting annually to senior executives in their organization on the effectiveness of their InfoSec Program, including the progress of any remedial actions.
- Appointing a CISO and/or ISSO to fulfill the responsibilities of the CIO in maintaining their InfoSec Program.
- Managing internal security reviews of the program business cases, alternatives analyses, and other specific investment documents.
- Managing and certifying an inventory of all current and proposed investments containing an IT component in accordance with the HHS Capital Planning and Investment Control (CPIC) process.
- Ensuring that policies, procedures, and practices are consistent with HHS and NIH requirements in order to ensure that programs, systems, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources, unintended release of HHS and NIH data, or denial of service (DoS).
- Ensuring that all employees and contractors comply with HHS, NIH and IC InfoSec Program IT security and privacy policies.
- Ensuring the establishment of a computer security incident response team (CSIRT) to participate in the investigation and resolution of incidents within their organization.
- Establishing, implementing, and enforcing an organization-wide framework to facilitate an incident response program (including PII and PHI breaches) that ensures proper and timely reporting to NIH Threat Mitigation and Incident Response (TMIR).
- Managing an inventory of all major information systems, devices and other items per FISMA requirements and as required by OMB.
- Ensuring mandatory security training, education, and awareness activities are undertaken by all personnel using, operating, supervising, or managing information systems.
- Exercising primary responsibility and authority for management of their security program.

- Developing a strategy for the continuous monitoring¹¹ of security control effectiveness and any proposed or actual changes to the information system and its environment of operation¹².
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.2 Chief Information Security Officer (CISO)¹³

The responsibilities of the CISO include, but are not limited to:

- Leading their InfoSec Program and promoting proper IT security and privacy practices.
- Supporting the NIH CISO in the implementation of the HHS Cybersecurity and NIH InfoSec Programs.
- Fostering communication and collaboration among the NIH and IC security and privacy stakeholders to share knowledge and to better understand threats to HHS and NIH information.
- Providing information about their InfoSec Program IT security and privacy policies to their management and throughout their organization.
- Providing advice and assistance to other organizational personnel concerning the security of sensitive information and of critical data processing capabilities.
- Advising the NIH CIO and their CIO about security-related incidents in accordance with the security breach reporting procedures developed and implemented by HHS and NIH.
- Disseminating information on potential security threats and recommended safeguards.
- Ensuring implementation of HHS, NIH, and IC policies and procedures that relate to IT security and privacy incident response and executing the responsibilities detailed in *NIH Policy Manual Chapter 1745-2, NIH Privacy and Information Security Incident and Breach Response Policy*.
- Collaborating with NIH Threat Mitigation and Incident Response (TMIR) when NIH TMIR is engaging their incident response team for information collection and clarification.

¹¹ The monitoring strategy may be included in the System Security Plan (SSP) to support the concept of near real-time risk management and ongoing authorization. The approval of the monitoring strategy may be obtained in conjunction with the SSP approval. The monitoring of security controls continues throughout the Enterprise Performance Life Cycle (EPLC).

¹² This is the responsibility of the System Owner or the Primary Operational IT Infrastructure Manager.

¹³ When an IC does have a CISO, the roles and responsibilities may fall the IC ISSO or a role designated by the IC CIO.

- Coordinating with the NIH Senior Official for Privacy (SOP) and their Privacy Coordinator to ensure privacy implications are addressed when PII incident response activities occur within their organization.
- Ensuring that roles with significant security responsibilities are identified and documented per the HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities.
- Conducting security education and awareness training needs assessments to determine appropriate training resources and to coordinate training activities for target populations.
- Supporting general privacy awareness and RBT activities for all personnel using, operating, supervising, or managing information systems.
- Assisting System Owners in establishing and implementing the required security safeguards to protect computer hardware, software, and data from improper use or abuse.
- Coordinating requirements for personnel clearances, position sensitivity, and access to information systems with the appropriate office.
- Establishing, documenting, and enforcing requirements and processes for granting and terminating all administrative privileges including, but not limited to, servers, security domains, and local workstations.
- Reviewing contracts for systems under their control to ensure that IT security is appropriately addressed in contract language.
- Auditing the processes above for effectiveness.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.3 Information System Security Officers (ISSO)

The responsibilities of each ISSO include, but are not limited to:

- Notifying the NIH CISO or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Serving as the focal point for IT security and privacy incident reporting and subsequent resolution.
- Ensuring that IT security notices and advisories are distributed to appropriate personnel and that vendor-issued security patches are installed in accordance with HHS and NIH directed timeframes.

- Assisting the NIH CISO and their IC CISO in reviewing contracts for systems under the NIH and/or IC CISO's control to ensure that IT security is appropriately addressed in contract language.
- Ensuring that security-related documentation at each phase of the Enterprise Performance Life Cycle (EPLC) meets all identified security needs.
- Maintaining the security documentation for systems under his or her purview, according to *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.
- Ensuring NIST SP 800-53, Rev 4 controls are appropriate to the system based on *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners and the NIH CISO in capturing all system weaknesses in the POA&M.
- Enforcing the concept of separation of duties by ensuring that no single individual has control of any critical process in its entirety per NIST SP 800-53, Rev 4.
- Participating in HHS and NIH required security Role-Based Training (RBT).
- Tracking all security education and awareness training conducted for personnel and contractors, as appropriate.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO, in coordination with the system/network administrators, in ensuring proper backup procedures exist for all system and network information.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in ensuring logical access controls are in place that provide protection from unauthorized access, alteration, loss, and disclosure of information.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in ensuring account lockout controls are in place that limit the number of consecutive failed log-in attempts against a given system.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in ensuring limits are established for the amount of time a session may be inactive before that session is timed out.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in ensuring that security-event monitoring technologies are used for all systems and networks.

- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in coordinating with Human Resources to manage physical and logical access controls for new and departing HHS or NIH employees and contractors.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in ensuring all incoming and outgoing connections from Department networks to the Internet, intranet, and extranets are made through a firewall.
- Assisting the CIO, CISO, System Owners, Data Owners, Business Owners, and NIH CISO in analyzing audit logs with the frequency defined by the NIH CISO and monitoring the types of assistance users request.
- Assisting Privacy Coordinator and IT System and TPWA Owner/Manager with the completing PIAs by answering any questions pertaining to security.
- Providing guidance and support within the IC to implement IT security controls that enhance privacy compliance.
- Ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the System Owner.
- Serving as a principal advisor to their CIO and CISO on matters involving the security of an information system.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.4 Privacy Coordinator

- Serves as the focal point within an IC for all privacy compliance-related activities.
- Serve as the liaison between IC staff and the NIH Office of the Senior Official for Privacy (OSOP) on privacy issues.
- Maintain awareness of Federal privacy laws and regulations to prevent the improper access, use or disclosure of PII (i.e., FOIA, Privacy Act, E-Gov, FISMA, HIPAA).
- Stay current on emerging technologies and their impact on personal privacy (i.e., mobile devices, social networking, cloud computing, health information exchange networks).
- Distribute strategic communications to IC staff so that they are informed of current privacy policies and procedures.
- Respond to requests for records stored in IC systems subject to the Privacy Act.

- Respond to OSOP data calls and requests for information (often generated by OMB and HHS).
- Foster the adoption of privacy policy and procedures and advise IC staff on all issues pertaining to privacy.
- Participate in the publication of System of Records Notices (SORNs).
- Attend the Privacy Coordinator Group (PCG) meetings.

3.2.5 *Security Control Assessor*

The responsibilities of the Security Control Assessor¹⁴ include, but are not limited to, the following for systems and networks under his or her authority:

- Assessing management, operational, and technical security controls employed within or inherited by an information system to evaluate the extent to which the controls are correctly implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Ensuring compliance with assessment requirements of NIH systems and networks under their authority.
- Ensuring the security authorization process is conducted in accordance with NIST guidance and HHS and NIH processes.
- Reviewing the system security documentation and results of the security control assessments and providing the results of the security control assessment (the security assessment report) in writing to the AO or AO Designated Representative.
- Providing an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
- Preparing the final security assessment report containing the results and findings from the assessment.
- Conducting, prior to initiating the security control assessment, an assessment of the System Security Plan (SSP) to ensure the plan provides a set of security controls for the information system that meet the stated security requirements.

¹⁴ There may be several Security Control Assessors supporting NIH and/or the ICs. NIH may designate or appoint a lead or primary Security Control Assessor to support the NIH AO. ICs may designate or appoint a lead or primary Security Control Assessor in their organization to support the CIO and/or CISO.

- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.6 *Program Executive*¹⁵

The responsibilities of the Program Executive include, but are not limited to:

- Ensuring that systems and information that are critical to the Program's mission receive adequate protection.
- Signing off on the FIPS 199 security categorization.
- Determining, in coordination with the Data Owner/Business Owner and System Owner, appropriate security controls and identifying resources to implement those controls.
- Coordinating system and data security requirements with IT security personnel by adequately delegating system-level security requirements.
- Ensuring that security for each information system is planned, documented, and integrated into the EPLC from the information system's initiation phase to the system's disposal phase.
- Ensuring adequate funding is provided to implement security requirements in the EPLC for systems that fall within the management authority of the Program Executive.
- Accepting reasonable risks, based on recommendations by the HHS CISO, NIH CISO, or the IC CISO and/or ISSO.
- Notifying the IC CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Ensuring that sensitive information and proprietary software is removed from IT equipment including printers, hard drives, and other memory devices prior to those items being offered for disposal or when a transfer of custody occurs.

3.2.7 *System Owner*

The responsibilities of the System Owner include, but are not limited to:

- Coordinating with the Contracting Officers (COs) and Contracting Officer's Representatives (CORs), Project Officers/Managers, CISO, ISSO and the NIH CISO to ensure that the appropriate security contracting language from the Health and Human Services Acquisition Regulation (HHSAR) and other relevant sources is incorporated in each IT contract.

¹⁵ A Program Executive is typically an individual responsible for budget, cost, scheduling, management, and performance of a specific program. This individual's title or position is generally defined by the organization where the program resides.

- Accepting accountability for the operation of a system(s) in support of the overall Program mission.
- Ensuring processing systems at facilities and IT utilities (ITUs) are certified at a level of security equal to or higher than the security level designated for their system.
- Ensuring that information and system categorization has been established for the system(s) and information under their purview in accordance with FIPS 199.
- Consulting with their CIO, CISO, ISSO, Privacy Coordinator, System Developers and Maintainers, and the Risk Executive (function) when establishing or changing system boundaries.
- Determining, in coordination with the Program Executive and Data Owner/Business Owner, appropriate security controls and identifying resources to implement those controls.
- Consulting with their CIO, CISO, ISSO and the NIH CIO or NIH CISO to establish consistent methodologies for determining IT security costs for systems.
- Ensuring that security for each information system is planned, documented, and integrated into the EPLC from the information system's initiation phase to the system's disposal phase.
- Ensuring provision of adequate funding to implement the security requirements in the EPLC for systems that fall within the management authority of the Program Executive.
- Ensuring that security-related documentation at each phase of the EPLC meets all identified security needs.
- Ensuring that all IT systems are configured in accordance with most recent Federal system security configuration guidance.
- Conducting Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs) on their system(s), in coordination with their respective Privacy Coordinator and the NIH SOP, pursuant to the AR-2 (Privacy Impact and Risk Assessment) Control described in the Privacy section.
- Serving as a POC for the system to whom privacy issues may be addressed.
- Collecting, modifying, using, and/or disclosing the minimum PII necessary to accomplish mission objectives.

- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Conducting assessments of the risk and magnitude of the harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the HHS and NIH critical operations, at no less than every three years or when significant changes occur to the system/network.
- Supporting the annual FISMA program reviews including the annual testing of security controls.
- Ensuring that system weaknesses are captured in the POA&M and are updated according to the HHS POA&M standard.
- Ensuring that sensitivity and criticality levels have been established for systems and information in accordance with NIST standards and guidelines.
- Ensuring proper physical, administrative, and technical controls are in place to protect PII if present on the system.
- Developing the System Security Plan (SSP) for system(s) and network(s) and documenting the security control implementation, as appropriate, in the SSP, and providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).
- Obtaining appropriate interconnection security agreements (ISAs) or memoranda of understanding (MOUs) prior to connecting with other systems and/or sharing sensitive data/information.
- Ensuring that system users and support personnel receive the requisite security training and developing system-specific rules of behavior (RoB) for systems under the System Owner's purview.
- Participating in HHS and NIH required security Role-Based Training (RBT).
- Determining who should be granted access to the system and with what rights and privileges and granting users the fewest possible privileges necessary for job performance in order to ensure privileges are based on a legitimate need.
- Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system.
- Enforcing the concept of separation of duties by ensuring that no single individual has control of the entirety of any critical process.

- Ensuring that special physical security or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk.
- Ensuring the development, execution, and activation of a system-to-system interconnection implementation plan for each instance of a system-to-system interconnection.
- Ensuring that sensitive information and proprietary software is removed from IT equipment (including printers), hard drives, and other memory devices prior to those items being offered for disposal or when a transfer of custody occurs.
- Accepting accountability for having an active security authorization for all deployed systems, to include pilot systems and retiring systems, assembling the authorization package and submitting it to the Authorizing Official (AO) and Authorizing Official Designated Representative.
- Developing a strategy for the continuous monitoring of security control effectiveness, and any proposed or actual changes to the information system and its environment of operation.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.8 *Data Owner/Business Owner*

The responsibilities of the Data Owner/Business Owner include, but are not limited to:

- Gathering, processing, storing, or transmitting HHS or NIH data in support of their ICs mission in accordance with HHS and NIH InfoSec Program policies and procedures.
- Ensuring that System Owners are aware of the sensitivity of data to be handled and ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data in accordance with FIPS 199 and FIPS 200.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.9 *Website Owner/Administrator*

The responsibilities of the Website Owner/Administrator include, but are not limited to:

- Coordinating Website privacy practices and compliance activities with the NIH Senior Official for Privacy (SOP).
- Ensuring that any NIH Website that employs a multi-session Web measurement and tracking technology that collects PII is approved by the NIH SOP and HHS Senior Agency Official for Privacy (SAOP) prior to its use.
- Ensuring that NIH Websites or NIH use of a third-party Website or application includes applicable privacy policies, privacy notices, and machine-readable privacy policies and that the content is accurate.

3.2.10 *Project/Program Manager*

The responsibilities of the Project/Program Manager include, but are not limited to:

- Evaluating proposals, if requested, to determine whether proposed security solutions effectively address agency requirements as detailed in acquisition documents.
- Ensuring that security-related documentation at each phase of the EPLC meets all identified security needs.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.

3.2.11 Contingency Planning Coordinator

The responsibilities of the Contingency Planning Coordinator include, but are not limited to:

- Developing the Contingency Plan (CP) strategy, in cooperation with other functional and resource managers associated with the system or the business processes supported by the system.
- Managing the development and execution of the CP.
- Coordinating with their CISO and/or ISSO and other key functional and resource managers to test the CP in accordance with NIST SP 800-53, Rev 4.
- Updating/maintaining all aspects of the CP.
- Ensuring that each team is trained and ready to deploy in the event of a disruptive situation requiring CP activation.
- Ensuring that recovery personnel are assigned to each team to respond to the event, recover capabilities, and return the system to normal operations.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.

3.2.12 System Developer and Maintainer

The responsibilities of the System Developer and Maintainer include, but are not limited to:

- Participating in HHS and NIH required security Role-Based Training (RBT)
- Integrating security into information systems from the onset of development, if possible.
- Ensuring that security-related documentation at each phase of the EPLC meets all identified security needs.
- Identifying laws and regulations relevant to the system's design and operation.
- Interpreting applicable laws and regulations into functional security requirements.
- Evaluating conflicting functional requirements to select for implementation those requirements that provide the highest level of security at the minimum cost consistent with applicable laws and regulations.
- Understanding the relationship between planned security safeguards and the features being installed on the system under development.

- Evaluating development efforts to ensure that baseline security safeguards are appropriately installed for systems in development or being modified.
- Participating in the construction of the information system in accordance with the formal design specifications, developing manual procedures, using commercial off-the-shelf (COTS) hardware/software components, writing program code, customizing hardware components, and/or using other IT capabilities.
- Designing and developing tests for security safeguard performance under a variety of normal and abnormal operating circumstances and workload levels.
- Analyzing system performance for potential security problems and providing direction to correct any problems identified during testing.
- Identifying security impacts associated with system implementation procedures.
- Leading the design, development, and modification of security safeguards to correct vulnerabilities identified during system implementation.
- Supporting assessments, reviews, evaluations, tests, and audits of the system by both internal and external entities.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Executing the Risk Management Framework (RMF) tasks in the *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

3.2.13 System/Network Administrator

The responsibilities of the System/Network Administrator include, but are not limited to:

- Participating in HHS and NIH required security Role-Based Training (RBT).
- Ensuring that the security posture of the network is maintained during all network maintenance, monitoring activities, installations or upgrades, and throughout day-to-day operations.
- Ensuring that appropriate security requirements are implemented and enforced for all systems or networks.
- Examining unresolved system vulnerabilities and determining which corrective action(s) or additional safeguards are necessary to mitigate the vulnerabilities.

- Implementing proper system backups, patching security vulnerabilities, and accurately reporting security incidents.
- Utilizing his or her “root” or “administrative” access rights to a computer on a “need-to-know” basis.
- Ensuring all incoming and outgoing connections from HHS and NIH networks to the Internet, intranet, and extranets are made through a firewall.
- Analyzing system performance for potential security problems.
- Conducting tests of security safeguards in accordance with the established test plan and procedures.
- Assessing the performance of security controls (to include hardware, software, firmware, and telecommunications, as appropriate) to ensure that the residual risk is within an acceptable range.
- Identifying security impacts associated with system implementation procedures.
- Leading the design, development, and modification of security safeguards to correct vulnerabilities identified during system implementation.
- Recognizing potential security violations and taking appropriate action to report any such incident as required by Federal regulation and mitigating any adverse impact.
- Developing and/or executing a system termination plan to ensure that security breaches are avoided during shutdown, and that the long-term protection of archived resources is achieved.
- Ensuring that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with the system termination plan.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.

3.2.14 Contracting Officer (CO) and Contracting Officer's Representative (COR)

The responsibilities of the CO and COR include, but are not limited to:

- Coordinating with the CIO, CISO, ISSO, System Owner, Data Owners, Business Owners, Project Officer/Manager, and the NIH CISO to ensure that the appropriate security and privacy contracting language from Health and Human Services Acquisition Regulation (HHSAR) and other relevant sources is incorporated in each IT contract.
- Determining the applicability of the Privacy Act when the design or development of a Privacy Act System of Record (SOR) is required to accomplish an NIH function.
- Advising contractors who develop or maintain a Privacy Act SOR on behalf of the Federal Government that the Privacy Act applies to them to the same extent that it applies to the government, per Section 552a(m) of the Privacy Act.
- Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes, while ensuring that all terms and conditions of the IT contract are met.
- Monitoring contract performance and reviewing deliverables for conformance with contract requirements related to IT security and privacy.
- Taking action as needed to ensure that accepted products meet contract requirements.
- Ensuring that sufficient funds are available for obligation per the Federal Acquisition Regulation (FAR).¹⁶
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.

¹⁶ FAR 1.602-1(b) states that no contract shall be entered into unless the CO ensures that all requirements of law, executive orders, regulations, and all other applicable procedures, including clearances and approvals, have been met.

3.2.15 *Supervisor*

The responsibilities of Supervisor include, but are not limited to:

- Ensuring compliance with IT security and privacy policies by all personnel under their direction, and providing the personnel, financial, and physical resources required to protect information resources appropriately.
- Budgeting resources for IT security training, including privacy and Role-Based Training (RBT), for personnel with security-related responsibilities (e.g., time, money, staff coverage).
- Ensuring that personnel under their direct report complete all required IT security training, including privacy and RBT, within the mandated timeframe.
- Notifying their appropriate CISO or ISSO and the NIH CISO, immediately of the unfriendly departure or separation of an HHS or NIH employee or contractor.
- Pursuing disciplinary or adverse actions against personnel and contractors who violate HHS policies or standards, including the HHS Rules of Behavior (RoB) and NIH-specific policies and procedures, including NIH General Rules of Behavior and any system-specific RoB.
- Preventing the disclosure of information retrieved from a Privacy Act System of Records (SORs), unless the record subject has given written consent to disclosure of his or her information, or the recipient is covered under the routine uses of disclosure of the Privacy Act Systems of Records Notice (SORN) or covered in one of the provisions found in 5 U.S.C. § 552a(b)(1)-(12) of the Privacy Act.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Verifying personnel security requirements are defined in the position description, the position description is reviewed annually for accuracy, and personnel security requirements are met for all employees.

3.2.16 *All Users*

The responsibilities of all HHS and NIH staff (employees, contractors, etc.), collectively users, operating on behalf of HHS or NIH include, but are not limited to:

- Reading, acknowledging, signing, and complying with the HHS Rules of Behavior (RoB), and/or the NIH General Rules of Behavior and any system-specific RoB, before gaining access to HHS or NIH systems and networks.
- Complying with all other HHS and NIH policies, standards, and procedures.

- Possessing awareness that they are not acting in an official capacity when using HHS and NIH IT resources for non-governmental purposes.
- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act data, copyright data, and procurement-sensitive information.
- Ensuring that all media containing HHS or NIH data is appropriately marked and labeled to indicate the sensitivity of the data.
- Abstaining from loading unapproved software from unauthorized sources¹⁷ on HHS or NIH systems or networks.
- Ensuring that sensitive information is not stored on laptop computers or other portable devices unless the data is secured using encryption standards commensurate with the sensitivity level of the data.
- Completing required privacy and security awareness training.
- Implementing specified security and privacy safeguards to prevent fraud, waste, or abuse of the systems, networks, and data they are authorized to use.
- Conforming to security policies and procedures that minimize the risk to HHS and NIH systems, networks, and data from malicious software and intrusions.
- Agreeing not to disable, remove, install with intent to bypass, or otherwise alter security or administrative settings designed to protect HHS and NIH IT resources.
- Ensuring that adequate protection is maintained on the user's workstation, including not sharing passwords with any other person, and logging out, locking, or enabling a password-protected screen saver before leaving the user's workstation.
- Notifying their CISO or ISSO, NIH CISO, or NIH Threat Mitigation & Incident Response (TMIR) of actual or suspected computer security-related incidents, including PII and PHI breaches.
- Seeking guidance from supervisors when in doubt about implementing this document.

¹⁷ An unauthorized source is any location (e.g., file store or server to which a device could connect, Internet site, intranet site) or process that is not permitted by HHS or NIH IT security personnel for the distribution of software.

4 Appendix B: Security Controls Section

This section closely follows *National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, Appendix F*, with an overlay of NIH-specific assignments and additions. This structured set of security controls provides the foundation for mitigating risk; protecting NIH information and information systems and serves as a roadmap for NIH and the ICs to use in identifying and implementing security controls concerning the entire information and information systems life cycles.

The control families are arranged in alphabetical and sequential order, and the tables are organized into the following columns: Control ID, Control Title, Control Description, and Selections & Assignments based on the corresponding FIPS 199 security categorizations of the system (Low, Moderate, High).

Ordinary-font text is derived directly from NIST SP 800-53, Rev 4, while HHS- and NIH-specific assignments are in **green text**. In some cases, controls may have supplemental guidance in the form of an italicized "Note" at the bottom of the Control Description box. Personnel should still consult NIST SP 800-53, Rev 4 Supplemental Guidance sections for more information if needed. Special terms used throughout the Handbook may also be found in the [Glossary](#).

Please note that the matrix only contains the security controls that applicable to the NIH InfoSec Program and IC InfoSec Programs. Security controls "Not Selected," "Withdrawn," or identified as "Not Applicable" are not included in the matrix. However, if a security is "Selected" for at least one FIPS 199 security categorization, but "Not Selected" for the other categorizations, it will still be included in the matrix.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.1 Access Control (AC)					
AC-1	Access Control Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Access control policy at least once every three (3) years.; and 2. Access control procedures at least once every three (3) years. <p><i>Note: NIH Policy regarding AC-1 is as follows in the remaining AC controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-2	Account Management	<p>The organization:</p> <ul style="list-style-type: none"> a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: NIH-defined information system account types are Primary, Secondary, Resource, Service, Training, and Shared. b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by an NIH or IC Administrative Officer or an Administrative Officer's Designated Representative for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with AC-2e, AC-2 c.e.2, AC-2 c.e.3, and AC-2 c.e.13; g. Monitors the use of information system accounts; 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-2	Account Management	<p>h. Notifies account managers:</p> <ol style="list-style-type: none"> 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; <p>i. Authorizes access to the information system based on:</p> <ol style="list-style-type: none"> 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; <p>j. Reviews accounts for compliance with account management requirements at least within every 365 days; and</p> <p>k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.</p>	Selected	Selected	Selected
AC-2 c.e.1 ¹⁸	Automated System Account Management	The organization employs automated mechanisms to support the management of information system accounts.	Not Selected	Selected	Selected

¹⁸ c.e. (Control Enhancement). For example, this entry is Control Enhancement 1 (c.e.1).

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-2 c.e.2	Removal of Temporary/Emergency Accounts	<p>The information system automatically disables temporary accounts after [Assignment 1], while emergency accounts should be removed after [Assignment 2].</p> <p><i>Note: Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local log-on accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates.</i></p>	<p>Selected (for Low systems, this does not need to be an automatic process)</p> <p>Assignment 1: 365 days or less.</p> <p>Assignment 2: 60 days or less.</p>	<p>Selected</p> <p>Assignment 1: 180 days or less.</p> <p>Assignment 2: 60 days or less.</p>	<p>Selected</p> <p>Assignment 1: 30 days or less.</p> <p>Assignment 2: 30 days or less.</p>
AC-2 c.e.3	Disable Inactive Accounts	<p>The information system automatically disables inactive accounts after 120 days or less.¹⁹</p>	<p>Not Selected</p> <p><i>Note: Selected only for administrator accounts.</i></p>	<p>Selected</p>	<p>Selected</p>
AC-2 c.e.4	Automated Audit Actions	<p>The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the information system account manager and/or the NIH Enterprise Directory (NED) management team.</p>	<p>Not Selected</p>	<p>Selected</p>	<p>Selected</p>
AC-2 c.e.5	Inactivity Logout	<p>The organization requires that users log out at the end of their normal work period.</p>	<p>Not Selected</p>	<p>Not Selected</p>	<p>Selected</p>

¹⁹ This control parameter is changed per NIH InfoSec Program GSS Waiver ID 20038.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-2 c.e.11	Usage Conditions	<p>The information system enforces the NIH-defined usage conditions in the HHS Rules of Behavior (RoB) for Use of Information and IT Resources Policy; NIH IT General Rules of Behavior; and NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment for the NIH information system account types defined in AC-2a.</p> <p><i>Note: Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.</i></p>	Not Selected	Not Selected	Selected
AC-2 c.e.12	Account Monitoring/ Atypical Usage	<p>The organization:</p> <ol style="list-style-type: none"> Monitors information system accounts for atypical use that is not associated with the use conditions in the HHS Rules of Behavior (RoB) for Use of Information and IT Resources Policy; NIH IT General Rules of Behavior; and NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment; and Reports atypical usage of information system accounts to the NIH CISO, IC ISSO or NIH ISAO. <p><i>Note: Atypical usage includes, for example, accessing information systems at times of the day and from locations that are not consistent with that user's normal usage patterns.</i></p>	Not Selected	Not Selected	Selected
AC-2 c.e.13	Disable Accounts for High-Risk Individuals	<p>The organization disables accounts of users posing a significant risk immediately after discovery of the risk.</p> <p><i>Note: Users posing a significant risk include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between AOs, network/system administrators, and HR managers is essential in order for timely execution of this control enhancement.</i></p>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-3	Access Enforcement	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Selected	Selected	Selected
AC-4	Information Flow Enforcement	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on least privilege and ISA/MOU information flow control policies for interconnected systems.	Not Selected	Selected	Selected
AC-5	Separation of Duties	<p>The organization:</p> <ul style="list-style-type: none"> a. Separates duties of individuals with role-based responsibilities and requires these individuals to complete Role-Based Training (RBT); b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. <p><i>Note: 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, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring system administrators do not also perform independent audit functions.</i></p>	Not Selected	Selected	Selected
AC-6	Least Privilege	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-6 c.e.1	Authorize Access to Security Functions	<p>The organization explicitly authorizes access to security functions (deployed in hardware, software, and firmware) and security-relevant information to include, at a minimum:</p> <ul style="list-style-type: none"> • Setting/modifying audit logs and auditing behavior; • Setting/modifying boundary protection system rules; • Configuring/modifying access authorizations (i.e., permissions, privileges); • Setting/modifying authentication parameters; and • Setting/modifying system configurations and parameters. 	Not Selected	Selected	Selected
AC-6 c.e.2	Non-Privileged Access for Non-Security Functions	<p>The organization requires that users of information system accounts, or roles, with access to standard user and non-security functions and information use non-privileged accounts, or roles, when accessing non-security functions. At a minimum, the NIH-defined controlled security functions include:</p> <ul style="list-style-type: none"> • Setting/modifying audit logs and auditing behavior; • Setting/modifying boundary protection system rules; • Configuring/modifying access authorizations (i.e., permissions, privileges); • Setting/modifying authentication parameters; and • Setting/modifying system configurations and parameters. 	Not Selected	Selected	Selected
AC-6 c.e.3	Network Access to Privileged Commands	<p>The organization authorizes network access to NIH services and resources by blocking all inbound network traffic at the security perimeter by NIH firewalls, with the exception of inbound traffic explicitly authorized to achieve the NIH mission and documents the rationale for such access in the System Security Plan (SSP) for the information system.</p> <p><i>Note: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).</i></p>	Not Selected	Not Selected	Selected
AC-6 c.e.5	Privileged Accounts	<p>The organization restricts privileged accounts on the information system to personnel or roles NIH identified as role-based personnel or roles that require Role-Based Training (RBT).</p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-6 c.e.9	Auditing Use of Privileged Functions	The information system audits the execution of privileged functions.	Not Selected	Selected	Selected
AC-6 c.e.10	Prohibit Non-Privileged Users from Executing Privileged Functions	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Not Selected	Selected	Selected
AC-7	Unsuccessful Logon Attempts	<p>The information system:</p> <ol style="list-style-type: none"> Enforces the following limits of consecutive invalid logon attempts by a user: [Assignment 1]. When the maximum number of unsuccessful attempts is exceeded, automatically [Assignment 2]. <p>Note: The above requirements for the maximum login attempts allowed when using ID and Password to authenticate to information systems. When authenticating with a PIV card, the maximum Personal Identification Number (PIN) attempts allowed for PIV cards is specified by policies implemented within the Smart Card Management System (SCMS) during issuance. These policies vary depending on a combination of card stock (64k, 128k), and certificate issuer for HHS (Cybertrust/Verizon Business CA or Entrust) and type of credential (PIV, RLA, ALT). The maximum allowed PIN attempts for each PIV card stock is as follows across all FISMA categories:</p> <ul style="list-style-type: none"> Fifteen (15) attempts – for 64k card stock in either Cybertrust / Verizon Business CA or those converted to Entrust certificates (64k card stock only); and Ten (10) attempts – for modern 128k cards issued by the Entrust CA. 	<p>Selected</p> <p>Assignment 1: for all users: five user/account attempts within 120 minutes.</p> <p>Assignment 2: locks the account/node for 15 minutes.</p>	<p>Selected</p> <p>Assignment 1: for all users: five user/account attempts within 120 minutes.</p> <p>Assignment 2: locks the account/node for 15 minutes.</p>	<p>Selected</p> <p>Assignment 1: for all users: three user/account attempts within 120 minutes.</p> <p>Assignment 2: locks the account/node until released by an administrator.</p>

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-8	System Use Notification	<p>The information system:</p> <ol style="list-style-type: none"> a. Displays to users the warning banner below before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance: <ol style="list-style-type: none"> 1. You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. 2. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. 3. By using this information system, you understand and consent to the following: <ol style="list-style-type: none"> i. You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. ii. Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-8	System Use Notification	<p><i>Note: At the recommendation of HHS OIG, should NIH or ICs need to add content to this sample warning banner, they should submit the modified warning banner language to OIG for review and approval prior to implementation. Also, in cases where NIH or ICs information systems have character limitations related to warning banner display, OIG can provide NIH and ICs with an abbreviated version of the warning banner. In some cases, the sample warning banner may be inconsistent with certain directives, policies, regulations, or standards (e.g., requirements governing special-purpose scientific or medical systems or tracking of personal information on publicly accessible Websites). In such cases, OpDivs should assess the applicability of the warning banner language and implement the warning banner where feasible and appropriate. To maintain consistency with NIST SP 800-53, any modified warning banner should contain the following content at a minimum:</i></p> <ol style="list-style-type: none"> <i>1. Users are accessing a U.S. Government information system;</i> <i>2. Information system usage may be monitored, recorded, and subject to audit;</i> <i>3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and</i> <i>4. Use of the information system indicates consent to monitoring and recording;</i> 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-8	System Use Notification	<p>b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and</p> <p>c. For publicly accessible systems:</p> <ol style="list-style-type: none"> 1. Displays system use information under the conditions in the NIH Public-facing Web Management Policy before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. <p>For public facing web pages to which the public has privileged access, e.g., clinical trial or adverse effects systems where users/patients are logging in to enter PII/PHI: You are accessing a U.S. Government web site which may contain information that must be protected under the U.S. Privacy Act or other sensitive information and is intended for Government authorized use only. Unauthorized attempts to upload information, change information, or use of this web site may result in disciplinary action, civil, and/or criminal penalties. Unauthorized users of this web site should have no expectation of privacy regarding any communications or data processed by this web site. Anyone accessing this web site expressly consents to monitoring of their actions and all communication or data transitioning or stored on or related to this web site and is advised that if such monitoring reveals possible evidence of criminal activity, NIH may provide that evidence to law enforcement officials.</p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-8	System Use Notification	For situations where the warning banner is subject to strict size restrictions, e.g., Oracle databases running on Solaris: This warning banner covers all devices/storage media attached to this system provided for Government authorized use only. Unauthorized/improper use is prohibited and may result in disciplinary action and/or civil and criminal penalties. At any time, and for any lawful Government purpose, the government may monitor, record, and audit your system usage and/or intercept, search, seize, disclose, or use any communication or data transiting or stored on this system. There is no reasonable expectation of privacy.	Selected	Selected	Selected
AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for each system account to one (1) session for normal users, and three (3) sessions for privileged users.	Not Selected	Not Selected	Selected
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after 15 minutes or less of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Not Selected	Selected	Selected
AC-11 c.e.1	Pattern-Hiding Displays	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Not Selected	Selected	Selected
AC-12	Session Termination	The information system automatically terminates a user session after the following condition or trigger event is detected: 30 minutes of inactivity.	Not Selected	Selected	Selected
AC-14	Permitted Actions Without Identification or Authentication	The organization: a. Identifies that no user actions can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the System Security Plan (SSP) for the information system, user actions not requiring identification or authentication.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-17	Remote Access	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed (including access to internal networks by VPN); b. Authorizes remote access to the information system prior to allowing such connections; and c. Access to HHS and/or NIH Webmail using personally-owned equipment is authorized. Access to other systems/networks using personally-owned equipment is prohibited without written authorization from the NIH or IC CIO, or an approved policy allowing the use of personally-owned equipment. If the NIH allows the use of personally-owned equipment on HHS or NIH systems or networks: <ul style="list-style-type: none"> 1. Personally-owned equipment must be scanned before being connected to HHS or NIH systems or networks to ensure compliance with HHS, NIH and IC system requirements (such as patch management requirements); and 2. Personally-owned equipment must be prohibited from processing, accessing, or storing HHS, NIH or IC sensitive information unless it is approved in writing by the NIH SOP and NIH CISO and employs FIPS 140-2-compliant encryption capabilities. <p><i>Note: In accordance with NIH Policy Manual Chapter 2814 – NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment, NIH phased out the use of Non-GFE in 2013. The content above is provided to preserve the integrity of the control as stated in NIST SP 800-53, Rev 4.</i></p>	Selected	Selected	Selected
AC-17 c.e.1	Automated Monitoring/ Control	The information system monitors and controls remote access methods.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-17 c.e.2	Protection of Confidentiality / Integrity Using Encryption	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, particularly when sending sensitive information (which must be protected with end-to-end encryption commensurate with the sensitivity level of the data).	Not Selected	Selected	Selected
AC-17 c.e.3	Managed Access Control Points	The information system routes all remote accesses through managed network access control points. NIH requires all remote accesses be managed through the NIH VPN or, with NIH CISO approval, remote access service must reside in a public-facing segment of DMZ.	Not Selected	Selected	Selected
AC-17 c.e.4	Privileged Commands/ Access	The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for unscheduled system administration and maintenance on critical systems required for time-sensitive operations or to respond to a cybersecurity incident when a time-sensitive response is a factor ; and b. Documents the rationale for such access in the System Security Plan (SSP) for the information system.	Not Selected	Selected	Selected
AC-18	Wireless Access	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; b. Authorizes wireless access to the information system prior to allowing such connections; and c. The organization ensures that: 1. NIH or IC CIOs approve and distribute the overall wireless plan for his or her respective organization ; 2. NIH and ICs adheres to the HHS Standard for IEEE 802.11 WLAN ; and 3. Mobile and wireless devices, systems, and networks are not connected to wired NIH, NIH or IC networks except through appropriate controls (e.g., VPN port) or unless specific authorization from HHS or NIH network management has been received.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-18 c.e.1	Authentication and Encryption	<p>The information system protects wireless access to the system using authentication of users and/or devices and encryption.</p> <p><i>Note: This control shall be selected for all baselines (low, moderate, high) to comply with NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) requirement for user authentication and encrypted communications using WPA-2 and NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, 2-factor authentication requirements for WLAN connectivity.</i></p>	Selected	Selected	Selected
AC-18 c.e.3	Disable Wireless Networking	<p>The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.</p> <p><i>Note: This control shall be selected for all baselines (low, moderate, high) to comply with NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) requirement for disabling all WLAN network interfaces in client devices that are not authorized for use.</i></p>	Selected	Selected	Selected
AC-18 c.e.4	Restrict Configuration by Users	<p>The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.</p> <p><i>Note: This control shall be selected for all baselines (low, moderate, high) to comply with NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) requirement for restricting user configuration.</i></p>	Selected	Selected	Selected
AC-18 c.e.5	Antennas/ Transmission Power Levels	<p>The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.</p> <p><i>Note: This control shall be selected for all baselines (low, moderate, high) to comply with NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) requirement for calibrating transmission power levels.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-19	Access Control for Mobile Devices	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes usage restrictions (including prohibiting unapproved software downloads), configuration requirements (including password-protection consistent with the Department’s password requirements, up-to-date system patches, current anti-virus software, and functionality that prevents automatic code execution), connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems. 	Selected	Selected	Selected
AC-19 c.e.5	Full Device/ Container-Based Encryption	<p>The organization employs FIPS 140-2 compliant full-disk encryption to protect the confidentiality and integrity of information on NIH government-furnished equipment (GFE) laptop computers and mobile devices.</p> <p><i>Note: Encryption parameters, requirements, and waivers must be documented in NIH or IC policy, pursuant to the HHS Standard for Encryption of Computing Devices and Information and applicable NIH and IC policies.</i></p> <p><i>Note: In the absence of a FIPS 140-2 compliant full-disk encryption solution for a particular platform, no sensitive information, including personally identifiable information (PII), can be stored on the platform even if the platform is considered GFE.</i></p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-20	Use of External Information Systems	<p>The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:</p> <ul style="list-style-type: none"> a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. <p><i>Note: Absent an agreement that establishes such terms, conditions, and trust relationships, employees and contractors are not to utilize unauthorized external information systems (such as personal email or personal online storage accounts) to conduct any HHS, NIH or IC business whatsoever. Authorized external information systems are either federally-owned, contracted for use by the HHS, NIH or IC, or approved for use pursuant to a HHS or NIH device policy.</i></p>	Selected	Selected	Selected
AC-20 c.e.1	Limits on Authorized Use	<p>The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:</p> <ul style="list-style-type: none"> a. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and System Security Plan (SSP); or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. 	Not Selected	Selected	Selected
AC-20 c.e.2	Portable Storage Devices	<p>The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.</p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AC-21	Information Sharing	<p>The organization:</p> <ul style="list-style-type: none"> a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for NIH or IC-specific research or scientific circumstances or conditions to enhance health, lengthen life, or reduce illness and disability. and b. Employs an NIH approved Interconnection Service Agreement (ISA) /Memorandum of Understanding (MOU) or other agreement to assist users in making information sharing/collaboration decisions. <p><i>Note: "Other agreements" may include Data Sharing Agreement; Data Use Agreement; Information Sharing Agreement; Material Transfer Agreement; Proprietary Information Agreement; Affiliation Agreement; or Teaming Agreement.</i></p>	Not Selected	Selected	Selected
AC-22	Publicly Accessible Content	<p>The organization:</p> <ul style="list-style-type: none"> a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.2 Awareness and Training (AT)					
AT-1	Security Awareness and Training Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Security awareness and training policy at least once every three (3) years; and 2. Security awareness and training procedures at least once every three (3) years. <p><i>Note: NIH Policy regarding AT-1 is as follows in the remaining AT controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AT-2	Security Awareness Training ²⁰	<p>The organization provides basic security and privacy awareness training to all information system users (including managers, senior executives, and contractors):</p> <ol style="list-style-type: none"> As part of initial training for new users; When required by system changes; and Annually thereafter. <p><i>Note: Users should also review and sign the Rules of Behavior for Use of HHS Information Resources (RoB) and NIH Information Technology General RoB when completing initial and annual refresher training (see PS-6).</i></p>	Selected	Selected	Selected
AT-2 c.e.2	Insider Threat	<p>The organization includes either in its annual security awareness training or in other annual supplemental training (such as a counterintelligence awareness course), information on recognizing and reporting potential indicators of insider threat, such as: inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. 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.</p> <p><i>Note: Periodic supplemental insider threat awareness activities are highly recommended, in addition to annual training.</i></p>	Not Selected	Selected	Selected

²⁰ At NIH, new hires must take the NIH Information Security Awareness Course and the NIH Privacy Awareness and Records Management Awareness Course. The annual refresher is a combined course called the Information Security, Counterintelligence, Privacy Awareness, Records Management Refresher.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
AT-3	Role-Based Security Training	<p>The organization provides role-based security-related training to all personnel with assigned significant responsibilities for information security:</p> <ul style="list-style-type: none"> a. Before authorizing access to the system or performing assigned duties; b. When required by system changes; and c. Within 60 days of entering a position that requires Role-Based Training (RBT), and at least annually thereafter. <p><i>Note: See Appendix F: Minimum Set of HHS and NIH Roles Assigned Significant Responsibilities for Information Security, which is directly related to this control.</i></p>	Selected	Selected	Selected
AT-4	Security Training Records	<p>For all users, the organization:</p> <ul style="list-style-type: none"> a. Documents and monitors individual information system security training activities including basic security awareness training, specific information system security training (if applicable and defined by the System Owner), and role-based security training; and b. Retains individual training records for a minimum of five (5) years after completing a specific training course. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-1	Audit and Accountability Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Audit and accountability policy at least once every three (3) years.; and 2. Audit and accountability procedures at least once every three (3) years. <p><i>Note: NIH Policy regarding AU-1 is as follows in the remaining AU controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-2	Audit Events	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events:</p> <ul style="list-style-type: none"> • Server alerts and error messages • User log-on and log-off (successful or unsuccessful) • System administration and privileged user activities; • Modification of privileges and access • Start up and shut down • Modifications to the application • Application alerts and error messages • Configuration changes • Account creation, modification, or deletion • Read access to sensitive information (System Category: Moderate and High only) • Modification to sensitive information System Category: Moderate and High only) • Printing sensitive information (System Category: Moderate and High only) <p>b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;</p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-2	Audit Events	<p>The organization:</p> <p>c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and</p> <p>d. Determines that events are to be audited within the information system at least weekly for, at a minimum,</p> <ul style="list-style-type: none"> • Unsuccessful log-on attempts that result in a locked account/node; • Configuration changes; • Application alerts and error messages; • System administration activities; • Modification of privileges and access; and • Account creation, modification, or deletion. <p><i>Note: These are the minimum set of events that should be audited, but ICs, System Owners, or applicable organization components are free to expand this list if necessary based on organizational risk.</i></p>	Selected	Selected	Selected
AU-2 c.e.3	Reviews and Updates	The organization reviews and, if necessary, updates the list of audited events within every 365 days and whenever there is a significant system modification.	Not Selected	Selected	Selected
AU-3	Content of Audit Records	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-3 c.e.1	Additional Audit Information	<p>The information system generates, if applicable, audit records containing the following additional information:</p> <ul style="list-style-type: none"> • Account Logon Events: Logon Success; Logon Failure (Failed User Authentication - Unknown user name or bad password; Multiple; Login Attempts/ Logon Failures: Account Locked Out); Logoff • Account Management: Account Created; Account Deleted; Account Disabled; Account Expired; Password Changed • Directory Service: Object (user, machine, etc.) Added to Domain/ Directory; Object Removed from Domain/ Directory; Domain Policy Change • Filesystem Events: Directory Created; Directory Deleted; Directory Read; Directory Write; Directory Permissions Changed; File Created; File Deleted; File Read; File Write; File Permissions Changed; Object Access • Logging Event: Event Log Full; Event Log Overwritten • Network Events: ACL Changed; Traffic Blocked at Firewall • Policy Change: All • Privilege Use: Privilege Escalation (i.e., Sudo); Privileged Object or Service Called; Object Accessed by Privileged Account • Process Tracking: Process Executed, Process Terminated; Scheduled Event Executed; Scheduled Event Failed • System Events: Service Stopped; System Startup; System Shutting Down; Session Disconnected 	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-3 c.e.2	Centralized Management of Planned Audit Record Content	The information system provides centralized management and configuration of the content to be captured in audit records, at a minimum, <ul style="list-style-type: none"> • NIH perimeter firewall; • Federal Information Security Management Act (FISMA) high categorized systems; • all NIH servers that provide web, database and network services/functions; and • security Infrastructure systems on the NIH network. 	Not Selected	Not Selected	Selected
AU-4	Audit Storage Capacity	The organization allocates audit record storage capacity, at a minimum, audit record storage capacity should be enough space to preserve 90 days of audit records.	Selected	Selected	Selected
AU-5	Response to Audit Processing Failures	The information system: <ol style="list-style-type: none"> a. Alerts NIH or IC System Administrators or System Owners in the event of an audit processing failure; and b. Takes additional actions, at a minimum, in the case of security audit log processing failure, information system processing must be halted (System Category: Moderate and High only). <p><i>Note: For Threat Mitigation & Incident Response (TMIR), Log Management, the NIH or IC ISSO and TMIR Log Management/Audit Administrators must be alerted.</i></p>	Selected	Selected	Selected
AU-5 c.e.1	Audit Storage Capacity	The information system provides a warning to NIH or IC System Administrator or System Owner and the NIH Data Center located on the main NIH Campus, IC managed Data Center, or contracted Data Center location, as applicable within 60 minutes when allocated audit record storage volume reaches 80% of maximum audit record storage capacity.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-5 c.e.2	Real-Time Alerts	<p>The information system provides an alert within 10 minutes to NIH or IC System Administrator or System Owner, IC ISSO, and NIH CISO, and the NIH Data Center located on the main NIH Campus, IC managed Data Center, or contracted Data Center location, as applicable when the following audit failure events occur:</p> <ul style="list-style-type: none"> • 50 or more failed logons within 10 minutes • Creation of user accounts outside NIH established process • Improper or unauthorized usage of administrator privileges • Use of service accounts for interactive log on • File access attempts by unauthorized user accounts • Deletion of files that user accounts have permission to access • Installation or execution of unapproved software • Access attempts with unauthorized devices • Hardware or software inventory change <p><i>Note: The above may be supplemented by IC CIOs and ISSOs to provide additional alerts related to their security requirements.</i></p>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-6	Audit Review, Analysis, and Reporting	<p>The organization:</p> <p>a. Reviews and analyzes information system audit records weekly for indications of</p> <ul style="list-style-type: none"> • Changes to sensitive system files • 50 or more failed logons within 10 minutes • Creation of user accounts outside NIH established process • Improper or unauthorized usage of administrator privileges • Use of service accounts for interactive log on • File access attempts by unauthorized user accounts • Deletion of files that user accounts have permission to access • Installation or execution of unapproved software • Access attempts with unauthorized devices • Hardware or software inventory change; and <p>b. Reports findings to the IC System Owner, IC CIO, IC ISSO, and NIH CISO.</p> <p><i>Note: The analysis of audit records must be integrated with analysis of vulnerability scanning information; system monitoring information; and data/information collected from other sources (as appropriate) to further enhance the ability to identify inappropriate or unusual activity. Information from audit records must be correlated with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.</i></p>	Selected	Selected	Selected
AU-6 c.e.1	Process Integration	The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	Not Selected	Selected	Selected
AU-6 c.e.3	Correlate Audit Repositories	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	Not Selected	Selected	Selected
AU-6 c.e.5	Integration/ Scanning and Monitoring Capabilities	The organization integrates analysis of audit records with analysis of data collected from other sources (e.g., vulnerability scanning information, performance data, information system monitoring information) to further enhance the ability to identify inappropriate or unusual activity.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-6 c.e.6	Correlation with Physical Monitoring	The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Not Selected	Not Selected	Selected
AU-7	Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	Not Selected	Selected	Selected
AU-7 c.e.1	Automatic Processing	<p>The information system provides the capability to process audit records for events of interest based on, at a minimum,</p> <ul style="list-style-type: none"> • Secured Target Name • Service Name • Event Server Time • User Name • Error Code • Event Name • Threat Severity • Target Object • Target Owner • Client Host Name • Network Connection • Secured Target Type • Policy Name • Event Time • Event Status • Error Message • Action Name • Log Cause • Target Type • OS User Name • Client IP • Client Program within audit records <p><i>Note: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals; event types; event locations; event times; event dates; system resources involved; IP addresses involved; or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.</i></p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-8	Time Stamps	<p>The information system:</p> <ul style="list-style-type: none"> a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and is synchronized to within two (2) seconds of the relative reference clock. <p><i>Note: Per NIST SP 800-53, Rev 4 guidance, it is best practice select a secondary time source that is in a different geographic region. However, this is not explicitly required by this control.</i></p>	Selected	Selected	Selected
AU-8 c.e.1	Synchronization with Authoritative Time Source	<p>The information system:</p> <ul style="list-style-type: none"> a. Compares the internal information system clocks at least quarterly with one or more of the federally-maintained Network Time Protocol (NTP) stratum 1 servers from either NIST (http://tf.nist.gov/tf-cgi/servers.cgi) or the U.S. Naval Observatory (http://tycho.usno.navy.mil/ntp.html); and b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than one (1) second. 	Not Selected	Selected	Selected
AU-9	Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Selected	Selected	Selected
AU-9 c.e.2	Audit Backup on Separate Physical Systems/Components	The information system backs up audit records weekly onto a physically different system or system component than the system or component being audited.	Not Selected	Not Selected	Selected
AU-9 c.e.3	Cryptographic Protection	The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	Not Selected	Not Selected	Selected
AU-9 c.e.4	Access by Subset of Privileged Users	The organization authorizes access to management of audit functionality to only NIH and IC System Administrators, System Owners, ISSOs, and CIO, NIH Threat Mitigation & Incident Response Team, and the NIH CISO.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-10	Non-Repudiation	<p>The information system protects against an individual (or process acting on behalf of an individual) falsely denying having, at a minimum, modified sensitive information records.</p> <p><i>Note: Non-repudiation provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message. For example: the use of PIV cards to digitally sign information is a common control that provides significant protection against repudiation.</i></p>	Not Selected	Not Selected	Selected
AU-11	Audit Record Retention	<p>The organization employs archiving measures to ensure that long-term audit records generated by the information system can be retrieved.</p> <p><i>Note: All audit logs must be retained in accordance with the following:</i></p> <ul style="list-style-type: none"> <i>The records schedule found in retention policy provided by the National Archives and Records Administration (NARA) General Records Schedules (GRS).</i> <i>Log files must be archived for a period of no less than 30 days (for low information systems), 180 days (for moderate information systems), and 365 days (for high information systems).</i> <i>Log files for remote access devices must be transferred from the devices to a central log server where they are retained for up to three (3) years.</i> <i>After being retained on the server for three years, they will be copied to optical permanent storage media where they will be retained in accordance with the records schedule associated with the system.</i> 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.3 Audit and Accountability (AU)					
AU-12	Audit Generation	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 (d), at a minimum, for Servers, Databases, Applications, and Network components (e.g., switches, routers); b. Allows NIH and IC System Administrators, System Owners, Network Administrators, ISSOs, CIO, and NIH Threat Mitigation & Incident Response Team and NIH CISO. to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	Selected	Selected	Selected
AU-12 c.e.1	Time-Correlated Audit Trail	The information system compiles audit records from at a minimum, for Servers, Databases, Applications, and Network components (e.g., switches, routers) into a system-wide (logical or physical) audit trail that is time-correlated to within one (1) minute of Coordinated Universal Time (UTC) format for consistency.	Not Selected	Not Selected	Selected
AU-12 c.e.3	Changes by Authorized Individuals	The information system provides the capability for NIH and IC System Administrators, System Owners, Network Administrators, Database Administrators, and ISSOs to change the auditing to be performed on at a minimum, Servers, Databases, Applications, and Network components (e.g., switches, routers) based on legitimate business needs that is documented in a formal change management process and the System Security Plan (SSP) and is approved by the NIH or IC CIO and ISSO or NIH CISO within 10 business days of the desired change.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.4 System Assessment and Authorization (CA)					
CA-1	Security Assessment and Authorization Policies and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Security assessment and authorization policy at least once every three (3) years; and 2. Security assessment and authorization procedures at least once every three (3) years <p><i>Note: NIH Policy regarding CA-1 is as follows in the remaining CA controls and control enhancements below.</i></p> <p><i>Note: All Department systems and networks must be formally assessed and authorized using the methods defined in NIST SP 800-37.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-2	Security Assessments	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops a security assessment plan that describes the scope of the assessment including: <ul style="list-style-type: none"> 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation within the scope of the system Security Assessment Plan (SAP), as defined by the Authorizing Official or their designated representative, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to the NIH or IC CIOs, ISSOs, Privacy Coordinator and System Owners, NIH OSOP, and NIH CISO. <p><i>Note: Consult NIST SP 800-53A, Rev 4 (a companion guideline to NIST SP 800-53, Rev 4) for specific guidance on the overall security assessment process, how to build effective security assessment plans, and how to analyze and manage assessment results.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-2 c.e.1	Independent Assessors	<p>The organization employs parameters of independence for assessors or assessment teams to conduct security control assessments.</p> <p><i>Note: The Authorizing Official determines (i) the required level of assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets, and to individuals; and (ii) if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.</i></p> <p><i>An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness. Independent assessors do not assess their own work; do not act as management or employees of the organizations they are serving; and do not place themselves in positions of advocacy for the organizations acquiring their services. Independent security control assessment services can be obtained from other components within the organization or can be contracted to a public or private sector entity outside of the organization. In special situations, for example, when the organization that owns the information system is small or the organizational structure requires that the security control assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the System Owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results.</i></p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-2 c.e.2	Specialized Assessments	The organization includes as part of security control assessments announced and unannounced penetration tests and annual Contingency Plan tests.	Selected	Selected	Selected
CA-2 c.e.3	External Organizations	The organization accepts the results of an assessment of 3rd party and contracted systems performed by an independent assessor when the assessment meets the requirements regarding eAuthorization categorization, FIPS 199 categories of information, vulnerabilities, and authorities to operate (ATO).	Not selected	Not selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-3	System Interconnections	<p>The organization:</p> <ol style="list-style-type: none"> Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements (ISAs) or data sharing agreements; Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and Reviews and, if necessary, updates ISAs at least once every calendar year and whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement. <p>The organization also considers the following actions:</p> <ul style="list-style-type: none"> Obtain written authorization from management (e.g., AO or designated representative) before connecting to other information systems. Consider that the terms and conditions of an ISA or data sharing agreement do not conflict with or otherwise contradict Department IT security and privacy policies, procedures, controls, and standards; applicable legislation, regulation, or guidance; or other contractual obligations. Ensure that system interconnection channels are securely configured commensurate with the confidentiality and integrity of the data being exchanged. Obtain authorization from the external System Owner if the Department intends to use, modify, or disclose the external system’s information in a manner not authorized by the agreement. 	Selected	Selected	Selected
CA-3 c.e.5	Restrictions on External System Connections	The organization employs a deny-all, permit-by-exception (i.e., whitelisting) policy for allowing NIH information systems to connect to external information systems.	Not selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-5	Plan of Action and Milestones	<p>The organization:</p> <ol style="list-style-type: none"> a. Develops a Plan of Action and Milestones (POA&M) in accordance with the HHS Standard for Plans of Action and Milestones (POA&M) Management and Reporting for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing POA&Ms at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. <p><i>Note: Findings resulting from a security assessment, audit, vulnerability scan, etc. shall be documented as weaknesses in a relevant POA&M after the assessment/final audit report is approved, or the vulnerability scan report is produced, whether applicable to a system or a program, and tracked until remediated/mitigated.</i></p> <p><i>Findings/weaknesses shall be documented in the POA&M and remediated/mitigated by the timelines below:</i></p> <ul style="list-style-type: none"> • <i>Critical within 30 days;</i> • <i>High within 60 days;</i> • <i>Medium within 1 year; and</i> • <i>Low within 1 year.</i> <p><i>For vulnerabilities detected by the Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS) team, remediation/mitigation timelines specified in the HHS Memorandum Remediation of High DHS-Discovered Scan Based Vulnerabilities shall be implemented.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-6	Security Authorization	<p>The organization:</p> <ul style="list-style-type: none"> a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization within every three (3) years or when there is a significant change to the system (defined as significant change that is likely to affect the security state of that information system)²¹. <p><i>Note: Organizations may conduct ongoing authorizations of information systems by implementing continuous monitoring programs (see CA-7). Continuous Diagnostics and Mitigation (CDM) programs can satisfy three-year reauthorization requirements, so that separate reauthorization processes may not be necessary. Also, although AOs will authorize the entire authorization package, organizations may wish to designate additional personnel to sign off on individual artifacts within the package (e.g. ITCP, risk assessment, ISA/MOU, etc.).</i></p>	Selected	Selected	Selected

²¹ Examples of such changes are provided in NIST SP 800-37, Section F.4 “Ongoing Authorization.”

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-7	Continuous Monitoring	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> a. Establishment of specific metrics to be monitored based on NIH security goals and objectives and in accordance with the basic requirements set forth in NIST SP 800-137; b. Establishment of at least monthly for monitoring and at least quarterly for assessments based on NIH security goals and objectives supporting such monitoring; c. Ongoing security control assessments in accordance with the NIH-specific continuous monitoring strategy; d. Ongoing security status monitoring of metrics defined in CA-7(a) in accordance with the NIH-specific continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of the organization and the information system to the NIH CIO and CISO and IC CIOs and ISSOs at least quarterly. <p><i>Note: HHS-level requirements for continuous monitoring (e.g., metrics, reporting frequencies and formats) will be defined as government-wide continuous monitoring requirements are established.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-7 c.e.1	Independent Assessment	<p>The organization employs independent assessors or assessment teams to monitor the security controls in the information system on an ongoing basis.</p> <p><i>Note: The Authorizing Official determines (i) the required level of assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets, and to individuals; and (ii) if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.</i></p>	Not Selected	Selected	Selected
CA-8	Penetration Testing	<p>The organization conducts penetration testing at least every two (2) years on high-profile or high-risk systems, as identified by the NIH CIO or CISO.</p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CA-9	Internal System Connections	<p>The organization:</p> <ul style="list-style-type: none"> a. Authorizes internal connections of network components and information system components (or classes of components) to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. c. The information system performs security compliance checks on constituent system components prior to the establishment of the internal connection. <p><i>Note: This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.5 Configuration Management (CM)					
CM-1	Configuration Management	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Configuration management policy at least every three (3) years; and 2. Configuration management procedures at least every three calendar (3) years. <p><i>Note: NIH Policy regarding CM-1 is as follows in the remaining CM controls and control enhancements below.</i></p>	Selected	Selected	Selected
CM-2	Baseline Configuration	<p>The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.</p> <p><i>Note: Baseline configurations are required for all systems and should be established during the implementation phase of every system. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-2 c.e.1	Reviews and Updates	The organization reviews and updates the baseline configuration of the information system: a. Assignment 1 for Moderate systems and Assignment 2 for High Systems; or b. When required due to interconnection modifications, critical security patches, upgrades, hardware replacements, emergency changes (such as those resulting from security incidents), significant system or environment changes, NIH or IC guideline changes, and other NIH or IC circumstances as appropriate; and c. As an integral part of information system component installations and upgrades.	Not Selected	Selected Assignment 1: Within every 365 days	Selected Assignment 2: Every six (6) months
CM-2 c.e.2	Automation Support for Accuracy/Currency	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	Not Selected	Not Selected	Selected
CM-2 c.e.3	Retention of Previous Configurations	The organization retains five (5) or more previous versions of the baseline configuration as deemed necessary by the NIH or IC CIO to support rollback.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-2 c.e.7	Configure Systems, Components, or Devices for High-Risk Areas	<p>The organization:</p> <ul style="list-style-type: none"> a. Issues government-furnished laptops and other mobile devices with FIPS 140-2 compliant encryption to individuals traveling to locations that the organization deems to be of significant risk; and b. Applies security safeguards (e.g., examining the device for physical tampering, purging or reimaging the hard disk drive) to the devices when the individuals return. <p><i>Note: In cases in which laptop encryption cannot be utilized to secure sensitive data (e.g., prohibition by United States export controls, travel to a country designated as high-risk per the HHS National Security Information Manual, potential danger, inability for personnel to perform work), a laptop that contains no sensitive information should be utilized. Refer to and follow OSSI guidelines for foreign travel.</i></p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-3	Configuration Change Control	<p>The organization:</p> <ul style="list-style-type: none"> a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for no less than twelve (12) months after the change; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through charted change control boards or other charted control bodies that convenes weekly and/or when configuration change conditions occur that require an unscheduled or emergency change. <p><i>Note: Change control boards should include the ISSO or their representative.</i></p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-3 c.e.1	Automated Document/ Notification/ Prohibition of Changes	The organization employs automated mechanisms to: a. Document proposed changes to the information system; b. Notify appropriate personnel (e.g., change control board or other control body, System Owner, project sponsor, ISSO, system administrator) of proposed changes to the information system and request change approval per the system configuration management documentation; c. Highlight proposed changes to the information system that have not been approved, deferred, or disapproved within a time period as defined by the system change management process, but no more than 60 days; d. Prohibit changes to the information system until designated approvals are received; e. Document all changes to the information system; and f. Notify appropriate personnel/roles (e.g., change control board or other control body, System Owner, project manager, ISSO, system administrator) when approved changes to the information system are completed.	Not Selected	Not Selected	Selected
CM-3 c.e.2	Test/ Validate/ Document Changes	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Not Selected	Selected	Selected
CM-4	Security Impact Analysis	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Selected	Selected	Selected
CM-4 c.e.1	Separate Test Environments	The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Not Selected	Not Selected	Selected
CM-5	Access Restrictions for Change	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-5 c.e.1	Automated Access Enforcement/ Auditing	The information system enforces access restrictions and supports auditing of the enforcement actions.	Not Selected	Not Selected	Selected
CM-5 c.e.2	Review System Changes	The organization reviews information system changes at least semi-annually and when so indicated by vulnerability scans, network scans, or other alerts and detection methods that an unauthorized change has occurred.	Not Selected	Not Selected	Selected
CM-5 c.e.3	Signed Components	The information system prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the NIH CIO or IC CIO.	Not Selected	Not Selected	Selected
CM-6	Configuration Settings	Per HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications, other configuration-related Department memoranda and standards, and any applicable NIH policy, the organization: a. Establishes and documents configuration settings for information technology products employed within the information system that using NIH and/or IC security configuration checklists reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings based on NIH and/or IC operational requirements; and d. Monitors and controls changes to the configuration settings.	Selected	Selected	Selected
CM-6 c.e.1	Automated Central Management/ Application/ Verification	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information system components as defined in the HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-6 c.e.2	Respond to Unauthorized Changes	The organization employs appropriate security safeguards (e.g., alerting designated organizational personnel, restoring established configuration settings, halting affected information system processing) to respond to unauthorized changes to information system components (e.g., authorization and/or auditing systems, system configuration baselines, log files, sensitive system libraries, executables) as defined by NIH, IC, or system, whichever is more restrictive.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-7	Least Functionality	<p>The organization:</p> <ul style="list-style-type: none"> a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of high-risk functions, ports, protocols, and/or services (e.g., Telnet, FTP). At a minimum, the following services must be specifically prohibited or restricted: <ul style="list-style-type: none"> • Domain Name System (DNS) <ul style="list-style-type: none"> ○ Port 53 / Transmission Control Protocol (TCP), User Datagram Protocol (UDP) • File Transfer Protocol (FTP) <ul style="list-style-type: none"> ○ Ports 20, 21 / TCP • Hypertext Transfer Protocol (HTTP) <ul style="list-style-type: none"> ○ Port 80 / TCP • Internet Message Access Protocol (IMAP) <ul style="list-style-type: none"> ○ Port 143 / TCP, UDP • Internet Relay Chat (IRC) <ul style="list-style-type: none"> ○ Port 194 / UDP • Network Basic Input Output System (NetBIOS) <ul style="list-style-type: none"> ○ Port 137 / TCP, UDP • Post Office Protocol 3 (POP3) <ul style="list-style-type: none"> ○ Port 110 / TCP • Remote Desktop Protocol (RDP) <ul style="list-style-type: none"> ○ Port 3389 / TCP • Network Time Protocol (NTP) <ul style="list-style-type: none"> ○ Port 123 / UDP • Secure Shell (SSH) <ul style="list-style-type: none"> ○ Port 22 / TCP 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-7	Least Functionality	<ul style="list-style-type: none"> • Server Message Block (SMB) <ul style="list-style-type: none"> ○ Ports 139 & 445 / TCP ○ Ports 137 & 138 / UDP • Session Initiation Protocol (SIP) <ul style="list-style-type: none"> ○ Port 5060 / TCP, UDP • Simple Mail Transfer Protocol (SMTP) <ul style="list-style-type: none"> ○ Port 25 / TCP • Simple Network Management Protocol (SNMP) <ul style="list-style-type: none"> ○ Port 161 / TCP, UDP • Structured Query Language (SQL) <ul style="list-style-type: none"> ○ Port 118 / TCP, UDP ○ Port 156 / TCP, UDP ○ Port 1433 / TCP ○ Port 1521 / TCP • Telnet <ul style="list-style-type: none"> ○ Port 23 / TCP 	Selected	Selected	Selected
CM-7 c.e.1	Periodic Review	The organization: <ol style="list-style-type: none"> a. Reviews the information system upon encountering a significant risk, or at least every 30 days, to identify unnecessary and/or non-secure functions, ports, protocols, and services; and b. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure. 	Not Selected	Selected	Selected
CM-7 c.e.2	Prevent Program Execution	The information system prevents program execution in accordance with HHS Rules of Behavior for Use of HHS Information and IT Resources Policy, NIH Information Technology General Rules of Behavior, associated individual IC Rules of Behavior, and, when necessary, rules authorizing the terms and conditions of software program usage.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-7 c.e.4	Unauthorized Software/ Blacklisting	<p>The organization:</p> <ul style="list-style-type: none"> a. Identifies a list of unauthorized software programs; b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and c. Reviews and updates the list of unauthorized software programs at least every 365 days, or, upon acquiring or discovering new software within the categories identified in CM-7(4)(a). <p><i>Note: Unauthorized software could include: software that is no longer supported by its vendor, compilers, known hacking tools, agents that support external file storage or data transmission, or unapproved VPN clients.</i></p>	Not Selected	Selected	Not Selected
CM-7 c.e.5	Authorized Software/ Whitelisting	<p>The organization:</p> <ul style="list-style-type: none"> a. Identifies a list of authorized software programs and rules authorizing the terms and conditions of software program usage in accordance with HHS Rules of Behavior for Use of HHS Information and IT Resources Policy, NIH Information Technology General Rules of Behavior, associated individual IC Rules of Behavior, and, when necessary, rules authorizing the terms and conditions of software program usage.; b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and c. Reviews and updates the list of authorized software programs at least every 180 days. 	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-8	Information System Component Inventory	<p>The organization:</p> <p>a. Develops and documents an inventory of information system components that:</p> <ol style="list-style-type: none"> 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes, at a minimum, information identified in Appendix G, System Component Inventory Requirements, and <p>b. Reviews and updates the information system component inventory in accordance with Assignment 1 for Low and Moderate systems and Assignment 2 for High systems.</p>	Selected Assignment 1: At least every 365 days	Selected Assignment 1: At least every 365 days	Selected Assignment 2: At least every 180 days
CM-8 c.e.1	Updates During Installations/Removals	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	Not Selected	Selected	Selected
CM-8 c.e.2	Automated Maintenance	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Not Selected	Not Selected	Selected
CM-8 c.e.3	Automated Unauthorized Component Detection	<p>The organization:</p> <p>a. Employs automated mechanisms at least weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and</p> <p>b. Takes the following actions when unauthorized components are detected:</p> <ul style="list-style-type: none"> • disables network access by such components, • isolates the components, and • notifies NIH CISO and IC System Owner, CIOs and ISSOs 	Not Selected	Selected	Selected
CM-8 c.e.4	Accountability Information	In the information system component inventory, the organization identifies by name, position and role individuals responsible/accountable for administering those components.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-8 c.e.5	No Duplicate Accounting of Components	The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	Not Selected	Selected	Selected
CM-9	Configuration Management Plan	<p>The organization develops, documents, and implements a configuration management plan for the information system that:</p> <ul style="list-style-type: none"> a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification. <p><i>Note: NIH and ICs must also ensure that personnel with configuration management responsibilities are trained on NIH, IC, or system applicable configuration management processes.</i></p>	Not Selected	Selected	Selected
CM-10	Software Usage Restrictions	<p>The organization:</p> <ul style="list-style-type: none"> a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CM-11	User-Installed Software	<p>The organization:</p> <ul style="list-style-type: none"> a. Prohibits the installation of software by users on all government-furnished equipment (GFE). b. Enforces software prohibition policies through: <ul style="list-style-type: none"> 1. the monthly examination of user accounts, 2. automated methods, and/or 3. the collection of application inventory controls; and c. Monitors policy compliance at least monthly. <p><i>Note: Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), collection of application inventory controls, or a combination of these methods.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.6 Contingency Planning (CP)					
CP-1	Contingency Planning Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Contingency planning policy at least every three calendar (3) years; and 2. Contingency planning procedures at least every three calendar (3) years. <p><i>Note: NIH Policy regarding CP-1 is as follows in the remaining CP controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-2	Contingency Plan	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops an information technology contingency plan (ITCP) in accordance with NIST SP 800-34 for all information systems that: <ul style="list-style-type: none"> 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles and responsibilities and assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed, approved, and signed by, at a minimum, the Contingency Plan Coordinator (CPC)²² and System Owner. b. Distributes copies of the ITCP to the CIO, ISSO, System Owner, CPC, system administrator, database administrator, business owner, and other personnel/roles, as appropriate; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the ITCP for the information system within every 365 days; e. Updates the ITCP to address changes to the organization, information system, or environment of operation and problems encountered during ITCP implementation, execution, or testing; f. Communicates ITCP changes to the CIO, ISSO, System Owner, CPC, system administrator, database administrator, business owner, and other personnel/roles, as appropriate; and g. Protects the ITCP from unauthorized disclosure and modification. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-2 c.e.1	Coordinate with Related Plans	The organization coordinates contingency plan development with organizational elements responsible for related plans. <i>Note: The organization should consider that ITCPs support Continuity of Operations Plans (COOP), particularly for information systems that support the continuity of the Department's critical business functions.</i>	Not selected	Selected	Selected
CP-2 c.e.2	Capacity Planning	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. <i>Note: Capacity planning is conducted and reviewed during the annual ITCP review.</i>	Not Selected	Not Selected	Selected
CP-2 c.e.3	Resume Essential Mission/ Business Functions	The organization plans for the resumption of essential missions and business functions within 24 hours of ITCP activation.	Not Selected	Selected	Selected
CP-2 c.e.4	Resume All Mission / Business Functions	The organization plans for the resumption of all missions and business functions within 24 hours of ITCP activation.	Not Selected	Not Selected	Selected
CP-2 c.e.5	Continue Essential Missions / Business functions	The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	Not Selected	Not Selected	Selected
CP-2 c.e.8	Identify Critical Assets	The organization identifies critical information system assets supporting essential missions and business functions.	Not Selected	Selected	Selected

²² The CPC may be the System Owner or their designated representative.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-3	Contingency Training	<p>The organization provides contingency training to personnel/roles with significant contingency responsibilities (as identified in the ITCP, per CP-2.a.3):</p> <ul style="list-style-type: none"> a. Within 60 days of assuming a contingency role or responsibility; b. When required by information system changes; and c. Within every 365 days thereafter. <p><i>Note: The organization formally tracks contingency training to ensure full coverage and compliance.</i></p>	Selected	Selected	Selected
CP-3 c.e.1	Simulated Events	The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Not Selected	Not Selected	Selected
CP-4	Contingency Plan Testing	<p>The organization:</p> <ul style="list-style-type: none"> a. Tests the ITCP for the information system at least every 365 days using NIST SP 800-34, NIST SP 800-84, exercises based on threat scenarios specific to an IC, system or region, and other tests and exercises, as appropriate to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the ITCP test results; and c. Initiates corrective actions, if needed. 	Selected	Selected	Selected
CP-4 c.e.1	Coordinate with Related Plans	The organization coordinates ITCP testing with organizational elements responsible for related plans.	Not Selected	Selected	Selected
CP-4 c.e.2	Alternate Processing Site	<p>The organization tests the ITCP at the alternate processing site:</p> <ul style="list-style-type: none"> a. To familiarize contingency personnel with the facility and available resources; and b. To evaluate the capabilities of the alternate processing site to support contingency operations. 	Not Selected	Not Selected	Selected
CP-6	Alternate Storage Site	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site. 	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-6 c.e.1	Separation from Primary Site	The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	Not Selected	Selected	Selected
CP-6 c.e.2	Recovery Time / Point Objectives	The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Not Selected	Not Selected	Selected
CP-6 c.e.3	Accessibility	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Not Selected	Selected	Selected
CP-7	Alternate Processing Site	The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within an allowable outage time consistent with the Recovery Time Objective (RTO) specified in the Business Impact Analysis (BIA) when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer, and resume operations are available at the alternate processing site or contacts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	Not Selected	Selected	Selected
CP-7 c.e.1	Separation from Primary Site	The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. <i>Note: The organization determines what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats identified during the risk assessment process (see RA-3).</i>	Not Selected	Selected	Selected
CP-7 c.e.2	Accessibility	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-7 c.e.3	Priority of Service	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). <i>Note: For high systems, recovery options must be configured in accordance with recovery time and recovery point objectives.</i>	Not Selected	Selected	Selected
CP-7 c.e.4	Preparation for Use	The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.	Not Selected	Not Selected	Selected
CP-8	Telecommunications Services	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of communication between Office of the Chief Information Officer (OCIO) and other organizations involved in coordination and support of the contingency plan and critical information systems used for essential missions and business functions within an allowable outage time consistent with the Recovery Time Objective (RTO) specified in the Business Impact Analysis (BIA) when the primary telecommunications capabilities are unavailable.	Not Selected	Selected	Selected
CP-8 c.e.1	Priority of Service Provisions	The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	Not Selected	Selected	Selected
CP-8 c.e.2	Single Point of Failure	The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-8 c.e.3	Separation of Primary/ Alternate Providers	The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Not Selected	Not Selected	Selected
CP-8 c.e.4	Provider Contingency Plan	The organization: <ul style="list-style-type: none"> a. Requires primary and alternate telecommunications service providers to have contingency plans; b. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and c. Obtains evidence of contingency testing/training by providers every 365 days. 	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-9	Information System Backup	<p>The organization:</p> <ul style="list-style-type: none"> a. Conducts backups of user-level information contained in the information system that is consistent with the Recovery Time Objective (RTO) and Recovery Point Objective in the Business Impact Analysis (BIA) where incremental backups must be executed at least weekly and full backups must be executed at least monthly; b. Conducts backups of system-level information contained in the information system that is consistent with the Recovery Time Objective (RTO) and Recovery Point Objective in the Business Impact Analysis (BIA) where incremental backups must be executed daily, and full backups must be executed at least weekly; c. Conducts backups of information system documentation including security-related documentation must be executed at least monthly; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations using cryptography (in the case of sensitive information) or other safeguards consistent with HHS, NIH, and IC policies. <p><i>Note: The organization ensures that one or more system backup strategies exist for the enterprise, are documented to support information system recovery, and meet the business continuity needs of the NIH and IC.</i></p>	Selected	Selected	Selected
CP-9 c.e.1	Testing for Reliability/ Integrity	The organization tests backup information at least semi-annually for Moderate systems and at least quarterly for High systems to verify media reliability and information integrity, and documents test results.	Not Selected	Selected	Selected
CP-9 c.e.2	Test Restoration Using Sampling	The organization uses a sample of backup information in the restoration of selected information system functions as part of ITCP testing.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
CP-9 c.e.3	Separate Storage for Critical Information	The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (i.e., hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.	Not Selected	Not Selected	Selected
CP-9 c.e.5	Transfer to Alternate Storage Site	The organization encrypts and transfers information system backup information to the alternate storage site on a schedule that is in accordance with the information systems' availability requirements and acceptable risk determination and at a rotation rate consistent with the RTO and RPO contained in the BIA. <i>Note: The use of encryption to safeguard backup information in transit must comply with HHS requirements for cryptographic protection (see SC-13).</i>	Not Selected	Not Selected	Selected
CP-10	Information System Recovery and Reconstitution	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	Selected	Selected	Selected
CP-10 c.e.2	Transaction Recovery	The information system implements transaction recovery for systems that are transaction-based.	Not Selected	Selected	Selected
CP-10 c.e.4	Restore within Time Period	The organization provides the capability to reimage information system components within the RTO and RPO contained in the BIA from configuration controlled and integrity-protected disk images representing a secure, operational state for the components.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.7 Identification and Authentication (IA)					
IA-1	Identification and Authentication Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Identification and authentication policy at least every three (3) years; and 2. Identification and authentication procedures at least every three (3) years. <p><i>Note: NIH Policy regarding IA-1 is as follows in the remaining CA controls and control enhancements below.</i></p>	Selected	Selected	Selected
IA-2	Identification and Authentication (Organizational Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Selected	Selected	Selected
IA-2 c.e.1	Network Access to Privileged Accounts	The information system implements multifactor authentication for network access to privileged accounts.	Selected	Selected	Selected
IA-2 c.e.2	Network Access to Non-Privileged Accounts	The information system implements multifactor authentication for network access to non-privileged accounts.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-2 c.e.3	Local Access to Privileged Accounts	The information system implements multifactor authentication for local access to privileged accounts.	Not Selected	Selected	Selected
IA-2 c.e.4	Local Access to Non-Privileged Accounts	The information system implements multifactor authentication for local access to non-privileged accounts.	Not Selected	Not Selected	Selected
IA-2 c.e.8	Network Access to Privileged Accounts – Replay Resistant	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. <i>Note: Replay-resistant techniques include, for example, protocols that use nonces²³ or challenges such as Transport Layer Security (TLS), and time synchronous, or challenge-response one-time authenticators.</i>	Not Selected	Selected	Selected
IA-2 c.e.9	Network Access to Non-Privileged Accounts – Replay Resistant	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts. <i>Note: Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS), and time synchronous, or challenge-response one-time authenticators.</i>	Not Selected	Not Selected	Selected

²³ In **cryptology**, a nonce is an arbitrary number that can only be used once. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an **authentication** protocol to ensure that old communications cannot be reused in replay attacks.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-2 c.e.11	Remote Access – Separate Device	<p>The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets strength of mechanism requirements consistent with:</p> <ul style="list-style-type: none"> • NIH Policy Manual Chapter 2810 – NIH Remote Access Policy; • NIH Wireless Network Security Standard; • NIH Mobile Device Security Standard; and/or • NIH CISO approved IC Remote Access Methods. 	Not Selected	Selected	Selected
IA-2 c.e.12	Acceptance of PIV Credentials	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.	Selected	Selected	Selected
IA-3	Device Identification and Authentication	The information system uniquely identifies and authenticates end user-operated devices (e.g. workstations, laptops, Voice over Internet Protocol (VoIP) phones, smartphones) and servers before establishing a local, remote, or network connection, which, at a minimum, use shared information (MAC or IP address) and access control lists to control remote network access before establishing a remote connection. If remote authentication is provided by the system itself, the system must be in compliance with OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-4	Identifier Management	The organization manages information system identifiers by: a. Receiving authorization from NIH or IC System Owner, ISSO, CIO, Authorizing Official, or Program Executive to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for three (3) years; and e. Disabling the identifier after Assignment 1, 2 or 3 depending on System Category, or fewer days at the discretion of the NIH CISO or IC CIO or ISSO, of inactivity.	Selected Assignment 1: 90 days	Selected Assignment 2: 60 days	Selected Assignment 3: 30 days
IA-5	Authenticator Management	The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-5	Authenticator Management	<p>d. Establishing and implementing administrative procedures for initial authenticator distribution (i.e., communicating passwords for encrypted files via a separate communication session rather than via the transmission of files themselves, such as sending one email with an encrypted file, and another email with the file password, etc.), for lost/compromised or damaged authenticators, and for revoking authenticators;</p> <p>e. Changing default content of authenticators prior to information system installation;</p> <p>f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;</p> <p>g. Changing/refreshing authenticators at the following intervals:</p> <ul style="list-style-type: none"> • Passwords – no longer than every 120 days²⁴, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords) • PIV Compliant Access Cards – no longer than every five (5) years • PKI certificates issued in accordance with Federal PKI Common Policy – no longer than every three (3) years <p>h. Protecting authenticator content from unauthorized disclosure and modification;</p> <p>i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and</p> <p>j. Changing authenticators for group/role accounts when membership to those accounts changes.</p> <p>k. “Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or certificate revocation list (CRL) to ensure that the certificate being used for authentication has not been revoked.</p>	Selected	Selected	Selected

²⁴ This control parameter is changed per NIH InfoSec Program GSS Waiver ID 19779.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-5 c.e.1	Password-Based Authentication	<p>The information system, for password-based authentication:</p> <p>a. Enforces minimum password complexity of at least one (1) character from each of the four (4) character categories (A-Z, a-z, 0-9, special characters), minimum length of eight (8) characters for regular user passwords, and minimum length of fifteen (15) characters for administrators or privileged users;</p> <p>Note: The minimum pin length for PIV Cards is at least six (6) digits.</p> <p>b. Enforces at least the following number of changed characters when new passwords are created: at least 75% of characters;</p> <p>c. Stores and transmits only encrypted representations of passwords;</p> <p>d. Enforces password minimum and maximum lifetime restrictions of: minimum password age of one (1) day and maximum password age of 120 days²⁵;</p>	Selected	Selected	Selected

²⁵ This control parameter is changed per NIH InfoSec Program GSS Waiver ID 19779.

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-5 c.e.1	Password-Based Authentication	<p>e. Prohibits password reuse for at least six (6) generations; and</p> <p>f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.</p> <p><i>Note: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., PIV cards). Also, administrator/privileged users are defined as those authorized for limited administrative purposes only based on business or technical need. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.</i></p>	Selected	Selected	Selected
IA-5 c.e.2	PKI-Based Authentication	<p>The information system, for PKI-based authentication:</p> <p>a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;</p> <p>b. Enforces authorized access to the corresponding private key;</p> <p>c. Maps the authenticated identity to the account of the individual or group; and</p> <p>d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.</p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-5 c.e.3	In-Person or Trusted Third-Party Registration	The organization requires that the registration process to receive all NIH administrative tokens and other credentials used for two-factor authentication be conducted in person before a designated registration authority with authorization by a designated organizational official (e.g., supervisor).	Not Selected	Selected	Selected
IA-5 c.e.11	Hardware Token-Based Authentication	The information system, for hardware token-based authentication, employs mechanisms that satisfy HHS-level PKI token quality requirements (e.g., Personal Identity Verification (PIV) cards. <i>Note: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular public key infrastructure (PKI).</i>	Selected	Selected	Selected
IA-6	Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. <i>Note: Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.</i>	Selected	Selected	Selected
IA-7	Cryptographic Module Authentication	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Selected	Selected	Selected
IA-8	Identification and Authentication (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to all Department systems and networks (unless a risk-based decision is made for a particular system that does not require non-organization user authentication).	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IA-8 c.e.1	Acceptance of PIV Credentials from Other Agencies	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. <i>Note: If NIH or an IC chooses to independently recognize PIV or CAC credentials from external federal agencies, this requires that NIH or the IC credential via Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) to be sure that the certificate is still valid prior to granting access.</i>	Selected	Selected	Selected
IA-8 c.e.2	Acceptance of Third-Party Credentials	The information system accepts only FICAM-approved third-party credentials. <i>Note: Federal Identity, Credential, and Access Management (FICAM)-approved path discovery and validation products and services are those products and services that have been approved through the FICAM conformance program, where applicable. Additional guidance is available at https://www.idmanagement.gov/.</i>	Selected	Selected	Selected
IA-8 c.e.3	Use of FICAM-Approved Products	The organization employs only FICAM-approved information system components in HHS and NIH information systems to accept third-party credentials.	Selected	Selected	Selected
IA-8 c.e.4	Use of FICAM-Issued Profiles	The information system conforms to FICAM-issued profiles.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.8 Incident Response (IR)					
IR-1	Incident Response Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, in accordance with the HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII) and HHS-OCIO Policy for IT Security and Privacy Incident Reporting and Response; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Incident response policy at least every three (3) years; and 2. Incident response procedures at least every three (3) years. <p><i>Note: NIH Policy regarding IR-1 is as follows in the remaining IR controls and control enhancements below.</i></p>	Selected	Selected	Selected
IR-2	Incident Response Training	<p>The organization provides incident response training to information system users consistent with assigned roles and responsibilities:</p> <ul style="list-style-type: none"> a. Within one (1) month of assuming an incident response role or responsibility. b. When required by information system changes; and c. At least once every 365 days thereafter. 	Selected	Selected	Selected
IR-2 c.e.1	Simulated Events	<p>The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.</p>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IR-2 c.e.2	Automated Training Environments	The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.	Not Selected	Not Selected	Selected
IR-3	Incident Response Testing	<p>The organization:</p> <ul style="list-style-type: none"> a. Tests the incident response capability for the information system annually using walk-throughs or tabletop exercises, simulations (parallel/full interrupt), or comprehensive exercises to determine the incident response effectiveness; and b. Documents the results. <p><i>Note: Testing must be scenario-based. At a minimum, tabletop exercises must be performed; however, more robust functional exercises are recommended.</i></p>	Not Selected	Selected	Selected
IR-3 c.e.2	Coordination with Related Plans	The organization coordinates incident response testing with organizational elements (e.g. physical security, emergency preparedness, response, and notification) responsible for related plans (e.g., Contingency Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans).	Not Selected	Selected	Selected
IR-4	Incident Handling	<p>The organization:</p> <ul style="list-style-type: none"> a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. 	Selected	Selected	Selected
IR-4 c.e.1	Automated Incident Handling Processes	The organization employs automated mechanisms to support the incident handling process.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IR-4 c.e.4	Information Correlation	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Not Selected	Not Selected	Selected
IR-5	Incident Monitoring	The organization tracks and documents information system security incidents.	Selected	Selected	Selected
IR-5 c.e.1	Automated Tracking/ Data Collection/ Analysis	The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	Not Selected	Not Selected	Selected
IR-6	Incident Reporting	The organization: a. Requires personnel to report suspected security incidents to the NIH Threat Mitigation & Incident Response (TMIR) within one (1) hour of discovery; and b. Report security incidents to the HHS Computer Security Incident Response Center (CSIRC) .	Selected	Selected	Selected
IR-6 c.e.1	Automated Reporting	The organization employs automated mechanisms to assist in the reporting of security incidents.	Not Selected	Selected	Selected
IR-7	Incident Response Assistance	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Selected	Selected	Selected
IR-7 c.e.1	Automation Support for Availability of Information/ Support	The organization employs automated mechanisms to increase the availability of incident response related information and support.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
IR-8	Incident Response Plan	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops an incident response plan that: <ul style="list-style-type: none"> 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by CIO and ISSO at the IC-level; b. Distributes copies of the incident response plan to NIH TMIR team and IC personnel with incident response responsibilities; c. Reviews the incident response plan at least annually; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to NIH TMIR team and IC personnel with incident response responsibilities; and f. Protects the incident response plan from unauthorized disclosure and modification. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.9 Maintenance (MA)					
MA-1	System Maintenance Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. System maintenance policy at least every three (3) years; and 2. System maintenance procedures at least every three (3) years. <p><i>Note: NIH Policy regarding MA-1 is as follows in the remaining MA controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MA-2	Controlled Maintenance	<p>The organization:</p> <ul style="list-style-type: none"> a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that NIH or IC System Owner explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes, at a minimum, the NIH-defined information points in the “Note” below in organizational maintenance records. <p><i>Note: For systems categorized as Moderate or High, maintenance records should include: (i) the date and time of maintenance; (ii) the name of the individual performing the maintenance; (iii) the name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed and replaced (including identification numbers, if applicable). For systems categorized as High, ensure automated mechanisms are employed to schedule, conduct, and document any maintenance and repairs as required.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MA-2 c.e.2	Automated Maintenance Activities	The organization: a. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and b. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.	Not Selected	Not Selected	Selected
MA-3	Maintenance Tools	The organization approves, controls, and monitors information system maintenance tools.	Not Selected	Selected	Selected
MA-3 c.e.1	Inspect Tools	The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	Not Selected	Selected	Selected
MA-3 c.e.2	Inspect Media	The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	Not Selected	Selected	Selected
MA-3 c.e.3	Prevent Unauthorized Removal	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no organizational information (particularly HHS, NIH or IC sensitive information) contained on the equipment; b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption from NIH CISO and Senior Official for Privacy (SOP) explicitly authorizing removal of the equipment from the facility.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MA-4	Nonlocal Maintenance	The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the System Security Plan (SSP) (SSP) for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	Selected	Selected	Selected
MA-4 c.e.1	Auditing and Review	The organization: a. Audits nonlocal maintenance and diagnostic sessions and other audit events consistent with HHS, NIH and IC policies ; and b. Reviews the records of the maintenance and diagnostic sessions.	Not Selected	Selected	Selected
MA-4 c.e.2	Document Nonlocal Maintenance	The organization documents in the System Security Plan (SSP) for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	Not Selected	Selected	Selected
MA-4 c.e.3	Comparable Security/ Sanitization	The organization: a. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or b. Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MA-5	Maintenance Personnel	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. 	Selected	Selected	Selected
MA-5 c.e.1	Individuals Without Appropriate Access	<p>The organization:</p> <ul style="list-style-type: none"> a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: <ul style="list-style-type: none"> 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. 	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MA-6	Timely Maintenance	The organization obtains maintenance support and/or spare parts for key information system components contained in the System Security Plan (SSP) within the applicable Recovery Time Objective (RTO) specified in the Business Impact Analysis or Contingency Plan.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.10 Media Protection (MP)					
MP-1	Media Protection Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Media protection policy at least every three (3) years; and 2. Media protection procedures at least every three (3) years. <p><i>Note: NIH Policy regarding MP-1 is as follows in the remaining MP controls and control enhancements below.</i></p>	Selected	Selected	Selected
MP-2	Media Access	<p>The organization restricts access to digital and non-digital media pursuant to Appendix H, Information System Media to NIH authorized personnel outlined in Appendix A, Roles and Responsibilities.</p>	Selected	Selected	Selected
MP-3	Media Marking	<p>The organization:</p> <ul style="list-style-type: none"> a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data; and b. Exempts information system media marking only with an NIH CIO and CISO approved wavier from marking as long as the media remains within NIH or IC controlled data centers. 	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MP-4	Media Storage	The organization: a. Physically controls and securely stores information system media pursuant to Appendix H, Information System Media within HHS, NIH or IC controlled offices and data centers ; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Not Selected	Selected	Selected
MP-5	Media Transport	The organization: a. Protects and controls information system media pursuant to Appendix H, Information System Media during transport outside of controlled areas using cryptography (in the case of sensitive information), or security safeguards in accordance with HHS, NIH, and IC policies commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data ; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.	Not Selected	Selected	Selected
MP-5 c.e.4	Cryptographic Protection	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	Not Selected	Selected	Selected
MP-6	Media Sanitization	The organization: a. Sanitizes information system media pursuant to Appendix H, Information System Media prior to disposal, release out of organizational control, or release for reuse using sanitization techniques and procedures in accordance with NIST SP 800-88 Rev 1, Appendix A-Minimum Sanitization Recommendations ; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
MP-6 c.e.1	Review/ Approve/ Track/ Document/ Verify	The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.	Not Selected	Not Selected	Selected
MP-6 c.e.2	Equipment Testing	The organization tests sanitization equipment and procedures within every 365 days to verify that the intended sanitization is being achieved.	Not Selected	Not Selected	Selected
MP-6 c.e.3	Nondestructive Techniques	The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: prior to initial use, loss of positive chain of custody, or when a device is connected to a lower assurance network/system based on FIPS 199 security categorization.	Not Selected	Not Selected	Selected
MP-7	Media Use	The organization restricts the use of information system media (e.g., magnetic tapes, external/removable hard disk drives, flash drives, CDs, DVDs) on HHS, NIH and IC information systems or system components using manual and automated safeguards. <i>Note: The use of portable storage devices in HHS, NIH and IC information systems when such devices have no identifiable owner (e.g., individuals, organizations, or projects) is prohibited.</i>	Selected	Selected	Selected
MP-7 c.e.1	Prohibit Use Without Owner	The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.11 Physical and Environmental Protection (PE)					
PE-1	Physical and Environmental Protection Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Physical and environmental protection policy at least every three (3) years; and 2. Physical and environmental protection procedures at least every three (3) years. <p><i>Note: NIH Policy regarding PE-1 is as follows in the remaining PE controls and control enhancements below.</i></p> <p><i>Note: NIH must document a facility System Security Plan (SSP) (or similar document) for the information system(s) residing therein that documents control for power equipment and cabling, emergency shutoff, emergency power, emergency lighting, fire protection, temperature and humidity controls, water damage protection, and delivery and removal of information systems-related items. This requirement applies to federally-owned, federally-leased, and contractor-operated facilities. NIH codifies this information in the NIH Data Center General Support System (GSS) System Security Plan (SSP).</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PE-2	Physical Access Authorizations	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals within every 365 days; and d. Removes individuals from the facility access list when access is no longer required. 	Selected	Selected	Selected
PE-3	Physical Access Control	<p>The organization:</p> <ul style="list-style-type: none"> a. Enforces physical access authorizations at entry/exit points to the facility where the information system resides by: <ul style="list-style-type: none"> 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards; b. Maintains physical access audit logs for entry/exit points; c. Provides security safeguards by verifying individual access authorization to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity for circumstances requiring visitor escorts and monitoring; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices within every 180 days for Low systems and every 90 days for Moderate and High systems; and g. Changes combinations and keys within every 365 days and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. 	Selected	Selected	Selected
PE-3 c.e.1	Information System Access	<p>The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at physical spaces containing one or more components of the information system.</p>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PE-4	Access Control for Transmission Medium	The organization controls physical access to information system distribution and transmission lines within organizational facilities using the following security safeguards: <ul style="list-style-type: none"> • Locked wiring closets • Disconnected or locked spare jacks • Protection of cabling by conduit or cable trays 	Not Selected	Selected	Selected
PE-5	Access Control for Output Devices	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Not Selected	Selected	Selected
PE-6	Monitoring Physical Access	The organization: <ol style="list-style-type: none"> a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs weekly and upon occurrence of events or indications of potential events in accordance with the note below; and c. Coordinates results of reviews and investigations with the organizational incident response capability. <p><i>Note: Examples of events that may initiate an investigative review process include: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and/or (iv) out-of-sequence accesses.</i></p>	Selected	Selected	Selected
PE-6 c.e.1	Intrusion Alarms/ Surveillance Equipment	The organization monitors physical intrusion alarms and surveillance equipment.	Not Selected	Selected	Selected
PE-6 c.e.4	Monitoring Physical Access to Information Systems	The organization monitors physical access to the information system in addition to the physical access monitoring of the facility to include physical spaces containing one or more components of the information system.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PE-8	Visitor Access Records	<p>The organization:</p> <ul style="list-style-type: none"> a. Maintains visitor access records to the facility where the information system resides (except for those areas officially designated as publicly accessible) for at least six (6) months; and b. Reviews visitor access records at least monthly, or, as defined in the NIH Infrastructure GSS SSP. <p><i>Note: At a minimum, visitor access records should include the following information:</i></p> <ul style="list-style-type: none"> 1. Name and organization of the person visiting; 2. Visitor's signature; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited. 	Selected	Selected	Selected
PE-8 c.e.1	Automated Records Maintenance/ Review	The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.	Not Selected	Not Selected	Selected
PE-9	Power Equipment and Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.	Not Selected	Selected	Selected
PE-10	Emergency Shutoff	<p>The organization:</p> <ul style="list-style-type: none"> a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices are located at the end of each row of racks for information systems or system components to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation. 	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PE-11	Emergency Power	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to a long-term alternate power source in the event of a primary power source loss.	Not Selected	Selected	Selected
PE-11 c.e.1	Long-Term Alternate Power Supply – Minimal Operational Capability	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Not Selected	Not Selected	Selected
PE-12	Fire Protection	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Selected	Selected	Selected
PE-13	Fire Protection	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Selected	Selected	Selected
PE-13 c.e.1	Detection Devices/ Systems	The organization employs fire detection devices/systems for the information system that activate automatically and notify NIH Center for Information Technology (CIT) Facilities and Infrastructure Services (FIS), NIH CIO, and NIH CISO and NIH Office of Research (ORS), Division of Fire and Rescue Services (DFRS) and NIH FIS emergency responders in the event of a fire.	Not Selected	Not Selected	Selected
PE-13 c.e.2	Suppression Devices/ Systems	The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to NIH CIT FIS, NIH CIO, and NIH CISO and NIH ORS DFRS and NIH FIS emergency responders.	Not Selected	Not Selected	Selected
PE-13 c.e.3	Automatic Fire Suppression	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PE-14	Temperature and Humidity Controls	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides within the limits as required by the equipment being protected ; and b. Monitors temperature and humidity levels in real time and continuously .	Selected	Selected	Selected
PE-15	Water Damage Protection	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Selected	Selected	Selected
PE-15 c.e.1	Automation Support	The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts NIH CIT FIS .	Not Selected	Not Selected	Selected
PE-16	Delivery and Removal	The organization authorizes, monitors, and controls types of information system components entering and exiting the facility and maintains records of those items.	Selected	Selected	Selected
PE-17	Alternate Work Site	The organization: a. Employs security controls and protections equivalent to the primary environment at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Not Selected	Selected	Selected
PE-18	Location of Information System Components	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards in accordance with the note below and to minimize the opportunity for unauthorized access. <i>Note: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation.</i>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.12 Planning (PL)					
PL-1	Security Planning Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Security planning policy at least every three (3) years; and 2. Security planning procedures at least every three (3) years. <p><i>Note: NIH Policy regarding PL-1 is as follows in the remaining PL controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PL-2	System Security Plan (SSP)	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops a System Security Plan (SSP) for the information system that: <ul style="list-style-type: none"> 1. Is consistent with the organization’s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the System Security Plan (SSP) and communicates subsequent changes to the plan to NIH CIO, CISO, System Owners, and NIH ISAO at the enterprise level and IC CIO, ISSO; System Owner, and IC InfoSec Program at the IC level. c. Reviews the System Security Plan (SSP) for the information system within every 365 days or when significant changes occur; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the System Security Plan (SSP) from unauthorized disclosure and modification. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PL-2 c.e.3	Plan/ Coordinate with Other Organizational Entities	<p>The organization plans and coordinates security-related activities affecting the information system with appropriate internal or external stakeholders, groups, or organizations before conducting such activities in order to reduce the potential impact on other organizational entities.</p> <p><i>Note: These stakeholders, groups, or organizations could include those involved with security-related activities, or providing services or support (such as TIC, or those involved in COOP planning). Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and CP/ITCP testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations.</i></p>	Not Selected	Selected	Selected
PL-4	Rules of Behavior	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes and makes readily available to individuals requiring access to the information system, the HHS Rules of Behavior (RoB) for Use of Information and IT Resources Policy, and the NIH Information Technology General Rules of Behavior – which define responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the HHS Rules of Behavior for Use of Information and IT Resources Policy, and the NIH Information Technology General Rules of Behavior, before authorizing access to information and the information system; c. Reviews and, if necessary, updates the HHS Rules of Behavior (RoB) for Use of Information and IT Resources Policy and the NIH Information Technology General Rules of Behavior at least every three (3) years; 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PL-4	Rules of Behavior	<p>d. Requires individuals who have signed a previous version of the HHS Rules of Behavior for Use of Information and IT Resources Policy and the NIH Information Technology General Rules of Behavior to read and re-sign on an annual basis or as needed, when the HHS Rules of Behavior for Use of Information and IT Resources Policy and the NIH Information Technology General Rules of Behavior are revised/updated; and</p> <p>e. Informs employees and contractors that the use of HHS information resources for anything other than authorized purposes set forth in the HHS Rules of Behavior for Use of Information and IT Resources Policy, and the NIH Information Technology General Rules of Behavior is a violation of either or both of those policies, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment.</p> <p><i>Note: NIH maintains its own NIH Information Technology General Rules of Behavior, which is based on the HHS Rules of Behavior and are no less restrictive. Usage of this RoB is permissible as a substitute for the HHS RoB. ICs may develop and enforce their own RoBs to accommodate their unique security and privacy requirement needs. IC RoBs cannot be less restrictive than HHS or NIH RoBs.</i></p> <p><i>In addition, a system-level RoB may also be required for some Moderate or High systems. These RoBs cannot be less restrictive than HHS or NIH RoBs.</i></p>	Selected	Selected	Selected
PL-4 c.e.1	Social Media and Networking Restrictions	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PL-8	Information Security Architecture	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops an information security architecture for the information system that: <ul style="list-style-type: none"> 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the Department’s enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture at least every three (3) years to reflect updates in the Department’s enterprise architecture; c. Ensures that planned information security architecture changes are reflected in the System Security Plan (SSP), the security Concept of Operations (CONOPS) (if applicable), and organizational procurements/acquisitions; and d. Ensures that the planned information security architecture is consistent with the Department’s enterprise architecture program and is based on the taxonomy of the Federal Enterprise Architecture (FEA). <p><i>Note: Consult the Common Approach to Federal Enterprise Architecture and other for federal enterprise architecture (FEA) guidance.</i></p>	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.13 Program Management (PM)					
PM-1	Information Security Program Plan	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops and disseminates an organization-wide information security program plan that: <ul style="list-style-type: none"> 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan at least every 365 days; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification. <p><i>Note: PM-1 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-2	Senior Information Security Officer	<p>The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.</p> <p><i>Note: PM-2 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PM-3	Information Security Resources	<p>The organization:</p> <ul style="list-style-type: none"> a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned. <p><i>Note: PM-3 is a Hybrid control and implementation and compliance is shared between the NIH InfoSec Program and the ICs' InfoSec Programs. The NIH ISAO complies with this control at the enterprise-level. ICs must comply with all elements of this control at the IC-level and provide the requisite data and information when requested from the NIH ISAO. The NIH ISAO must compile the data and information and provide an enterprise-level view when requested by NIH and other Government entities.</i></p>	Selected	Selected	Selected
PM-4	Plan of Actions and Milestones Process	<p>The organization:</p> <ul style="list-style-type: none"> a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: <ul style="list-style-type: none"> 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with OMB FISMA reporting requirements. b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. <p><i>Note: PM-4 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PM-5	Information Systems Inventory	<p>The organization develops and maintains an inventory of its information systems.</p> <p><i>Note: PM-5 is a Hybrid control and implementation and compliance is shared between the NIH InfoSec Program and the ICs' InfoSec Programs. This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. The NIH ISAO complies with this control at the enterprise-level. ICs must develop and maintain inventories for IC assets and resources and provide the requisite data and information when requested from the NIH ISAO. The NIH ISAO must compile the data and information and provide an enterprise-level view when requested by NIH and other Government entities.</i></p>	Selected	Selected	Selected
PM-6	Information Security Measures of Performance	<p>The organization develops, monitors, and reports on the results of information security measures of performance.</p> <p><i>Note: PM-6 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-7	Enterprise Architecture	<p>The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.</p> <p><i>Note: PM-7 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PM-8	Critical Infrastructure Plan	<p>The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.</p> <p><i>Note: PM-8 is a Hybrid control and implementation and compliance is shared between the NIH InfoSec Program and the ICs' InfoSec Programs. Protection strategies are based on the prioritization of critical assets and resources. The NIH ISAO complies with this control at the enterprise-level. ICs must develop protection strategies based on the prioritization of critical IC assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance such as Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience and the National Infrastructure Protection Plan (NIPP).</i></p>	Selected	Selected	Selected
PM-9	Risk Management Strategy	<p>The organization:</p> <ol style="list-style-type: none"> a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy at least every 365 days or as required, to address organizational changes. <p><i>Note: PM-9 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PM-10	Security Authorization Process	<p>The organization:</p> <ul style="list-style-type: none"> a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program. <p><i>Note: PM-10 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-11	Mission/Business Process Definition	<p>The organization:</p> <ul style="list-style-type: none"> a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. <p><i>Note: PM-11 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-12	Insider Threat Program	<p>The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.</p> <p><i>Note: PM-12 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-13	Information Security Workforce	<p>The organization establishes an information security workforce development and improvement program.</p> <p><i>Note: PM-13 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PM-14	Testing, Training, and Monitoring	<p>The organization:</p> <ul style="list-style-type: none"> a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: <ul style="list-style-type: none"> 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. <p><i>Note: PM-14 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-15	Contacts with Security Groups and Associations	<p>The organization establishes and institutionalizes contact with selected groups and associations within the security community:</p> <ul style="list-style-type: none"> a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents. <p><i>Note: PM-15 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected
PM-16	Threat Awareness Program	<p>The organization implements a threat awareness program that includes a cross-organization information-sharing capability.</p> <p><i>Note: PM-16 is a Common control, which is fully inherited from the NIH InfoSec Program.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.14 Personnel Security (PS)					
PS-1	Personnel Security Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Personnel security policy at least every three (3) years; and 2. Personnel security procedures at least every three (3) years. <p><i>Note: NIH Policy regarding PS-1 is as follows in the remaining PS controls and control enhancements below.</i></p> <p><i>Note: Refer to existing HHS and HHS Office of Security and Strategic Information (OSSI personnel security procedures and guidance for additional personnel security and suitability responsibilities.</i></p>	Selected	Selected	Selected
PS-2	Position Risk Designations	<p>The organization:</p> <ul style="list-style-type: none"> a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions: <ul style="list-style-type: none"> 1. Ensures that all individuals with significant security responsibilities possess, at a minimum, a Level 5 Public Trust; 2. Ensures that individuals are designated to position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position; and c. Reviews and, if necessary, updates position risk designations at least within three (3) years or whenever a position’s duties are changed/revised/realigned and ensures that these risk designations are consistent with U.S. Office of Personnel Management (OPM) policy and guidance. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PS-3	Personnel Screening	The organization: <ol style="list-style-type: none"> a. Screens individuals prior to authorizing access to the information system; b. Rescreens individuals anytime they move to a new position with a higher risk designation; c. Conducts background investigations in a manner commensurate with OPM and HHS Human Resources policy and guidance; d. Performs reinvestigations in accordance with guidance provided by current personnel security policy; and e. Refuses employees and contractors access to information systems until they have: <ol style="list-style-type: none"> 1. Been granted an interim clearance, and 2. Signed the appropriate access agreements. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PS-4	Personnel Termination	<p>The organization, upon termination of individual employment:</p> <ul style="list-style-type: none"> a. Disables information system access as soon as possible but no longer than seven (7) calendar days following termination or, if necessary, prior to the formal termination action; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of continued obligations under information systems non-disclosure, confidentiality, and user access agreements; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies the appropriate NIH Facilities and Infrastructure Services (FIS); Human Resources; information systems management, supervisors, and administrators; and physical security personnel within seven (7) calendar days of the individual’s termination. <p><i>Note: NIH must retain for a reasonable time period, not less than the period available for the employee to appeal the termination, all electronic documentation in a central location, which can readily be retrieved in the event of litigation at a later date after a terminated employee has departed.</i></p>	Selected	Selected	Selected
PS-4 c.e.2	Automated Notification	<p>The organization employs automated mechanisms to notify the appropriate NIH Facilities and Infrastructure Services (FIS); Human Resources; information systems management, supervisors, and administrators; and physical security personnel upon termination of an individual.</p> <p><i>Note: If automated mechanisms are not feasible, a manual and documented process must be in place consistent with the baseline PS-4(f) control.</i></p>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PS-5	Personnel Transfer	<p>The organization:</p> <ul style="list-style-type: none"> a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to a new position within the organization; b. Initiates the re-evaluation of that individual’s logical and physical access controls as soon as possible, no later than 30 days of the formal transfer action; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies the appropriate NIH Facilities and Infrastructure Services (FIS); Human Resources; information systems management, supervisors, and administrators; and physical security personnel within 30 days of the formal transfer action. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PS-6	Access Agreements	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops and documents access agreements for organizational information systems; b. Reviews and, if necessary, updates the access agreements within every 365 days; and c. Ensures that individuals requiring access to organizational information and information systems: <ul style="list-style-type: none"> 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or within every 365 days. <p><i>Note: The Rules of Behavior for Use of HHS Information Resources (HHS RoB) is the standard HHS access agreement. All new users of HHS information resources must read the HHS RoB or NIH Information Technology General RoB and sign the accompanying acknowledgement form before accessing HHS, NIH or IC data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter, which is part of the NIH Information Systems Security Awareness Training (see AT-2).</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PS-7	Third-Party Personnel Security	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes third-party personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify the NIH or IC Contracting Office, Contracting Office Representative (COR), Federal Lead and federal employee operational manager of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges in accordance with Assignment 1, 2, or 3 depending on system category; and e. Monitors provider compliance. <p><i>Note: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.</i></p>	<p>Selected</p> <p>Assignment 1: As soon as possible within a maximum of 30 days from the formal transfer or termination action.</p>	<p>Selected</p> <p>Assignment 2: As soon as possible within a maximum of 7 days from the formal transfer or termination action.</p>	<p>Selected</p> <p>Assignment 3: As soon as possible within a maximum of 72 hours from the formal transfer or termination action.</p>

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
PS-8	Personnel Sanctions	<p>The organization:</p> <p>a. Employs a formal sanctions process (that may include termination of employment; removal or disbarment from work on federal contracts or projects; suspension of access privileges; revocation of access to federal information, information systems and/or facilities; criminal penalties) for individuals failing to comply with established information security policies and procedures; and</p> <p>b. Notifies the appropriate NIH or IC Contracting Office, Contracting Office Representative (COR), Federal Lead and federal employee operational manager within the Assignment 1, 2, or 3 parameters depending on system category when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.</p> <p><i>Note: appropriate personnel can include human resources managers/supervisors, system administrators, and physical security personnel.</i></p>	<p>Selected</p> <p>Assignment 1: As soon as possible within a maximum of 30 days</p>	<p>Selected</p> <p>Assignment 2: As soon as possible within a maximum of 7 days</p>	<p>Selected</p> <p>Assignment 3: As soon as possible within a maximum of 72 hours</p>

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.15 Risk Assessment (RA)					
RA-1	Risk Assessment Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. Risk assessment policy at least every three (3) years; and 2. Risk assessment procedures at least every three (3) years. <p><i>Note: NIH Policy regarding RA-1 is as follows in the remaining RA controls and control enhancements below.</i></p>	Selected	Selected	Selected
RA-2	Security Categorization	<p>The organization:</p> <ul style="list-style-type: none"> a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the System Security Plan (SSP) for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
RA-3	Risk Assessment	<p>The organization:</p> <ul style="list-style-type: none"> a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Conducts an e-Authentication Risk Assessment (ERA), as required on systems and determine e-authentication assurance levels and documents risk assessment results in the e-Authentication Risk Threshold/e-Authentication Risk Assessment (ETA/ERA, System Security Plan (SSP), Business Impact Assessment (BIA), Contingency Plan (CP), and Security Assessment Report (SAR); c. Reviews risk assessment results within every 365 days or when there are significant changes to the system or environment, whichever comes first; d. Disseminates risk assessment results to NIH CISO, NIH ISAO, NIH OSOP, and System Owner and IC CIO, ISSO, Privacy Coordinator, and System Owner; and e. Updates the risk assessment report before issuing a new Authority to Operate (ATO), or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system, or if none of these events occur, every three (3) years. <p><i>Note: The annual review of the risk assessment results should be documented and acknowledged by the System Owner.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
RA-5	Vulnerability Scanning	<p>The organization:</p> <ul style="list-style-type: none"> a. Scans for vulnerabilities in the information system and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: <ul style="list-style-type: none"> 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities and in accordance with an NIH or IC risk assessment and per HHS and/or NIH policies e. Shares information obtained from the vulnerability scanning process and security control assessments with to NIH CISO, NIH ISAO, NIH OSOP, and System Owner and IC CIO, ISSO, Privacy Coordinator, and System Owner; to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). <p><i>Note: The organization needs to have a documented process for vulnerability scanning with identified roles and responsibilities, incorporating appropriate federal oversight and separation of duties.</i></p>	Selected	Selected	Selected
RA-5 c.e.1	Update Tool Capability	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	Not Selected	Selected	Selected
RA-5 c.e.2	Update by Frequency/Prior to New Scan/When Identified	The organization updates the database of known information system vulnerabilities to be used in the scanning process at least every 30 days, immediately prior to a new scan, or when new vulnerabilities are identified and reported.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
RA-5 c.e.4	Discoverable Information	The organization determines what information about the information system is discoverable by adversaries and subsequently takes NIH- and IC-designated corrective actions.	Not Selected	Not Selected	Selected
RA-5 c.e.5	Privileged Access	The information system implements privileged access authorization to NIH and IC lists of information system components to facilitate more thorough vulnerability scanning and protect the sensitive nature of the scanning output.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.16 Systems and Services Acquisition (SA)					
SA-1	System and Services Acquisition Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. System and services acquisition policy at least every three (3) years; and 2. System and services acquisition procedures at least every three (3) years. <p><i>Note: NIH Policy regarding SA-1 is as follows in the remaining SA controls and control enhancements below.</i></p>	Selected	Selected	Selected
SA-2	Allocation of Resources	<p>The organization:</p> <ul style="list-style-type: none"> a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-3	System Development Life Cycle	<p>The organization:</p> <ul style="list-style-type: none"> a. Manages the information system using a formally defined and documented system development life cycle (SDLC) process that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the SDLC; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into SDLC activities. <p><i>Note: The organization may formally define and document its own SDLC process; however, at a minimum, the process must conform to HHS Department-wide SDLC requirements (including the HHS Enterprise Performance Life Cycle (EPLC)). The organization may adopt the Department-wide SDLC or customize it to meet additional, organization-specific requirements.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-4	Acquisition Process	<p>The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:</p> <ol style="list-style-type: none"> Security functional requirements; Security strength requirements; Security assurance requirements; Security-related documentation requirements; Requirements for protecting security-related documentation; Description of the information system development environment and environment in which the system is intended to operate; and Acceptance criteria. <p><i>Note: Required security configurations and settings should also be included (see SA-4 c.e.5).</i></p>	Selected	Selected	Selected
SA-4 c.e.1	Functional Properties of Security Controls	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	Not Selected	Selected	Selected
SA-4 c.e.2	Design/ Implementation Information for Security Controls	<p>The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes one or more of the following:</p> <ul style="list-style-type: none"> Security-relevant external system interfaces; Source code or hardware schematics; Other NIH and/or IC design/implementation information at an NIH and/or IC level of detail 	Not Selected	Selected	Selected
SA-4 c.e.9	Functions/ Ports/ Protocols/ Services in Use	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-4 c.e.10	Use of Approved PIV Products	The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	Selected	Selected	Selected
SA-5	Information System Documentation	<p>The organization:</p> <ul style="list-style-type: none"> a. Obtains administrator documentation for the information system, system component, or information system service that describes: <ul style="list-style-type: none"> 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: <ul style="list-style-type: none"> 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and recreates selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to NIH and/or IC System Owners, System Administrators, Network Administrators, Data Owners, Business Owners, Project Managers, Service Area Managers, and other personnel as appropriate. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-8	Security Engineering Principles	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Not Selected	Selected	Selected
SA-9	External Information System Services	The organization: <ul style="list-style-type: none"> a. Requires that providers of external information system services comply with organizational information security requirements and employ HHS, NIH, and IC security controls and comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Formally defines and documents government oversight and user roles and responsibilities with regard to external information system services in a service level agreement (SLA) or similar agreement; and c. Employs processes, methods, and techniques as documented in contracts, service level agreements, and other agreements to monitor security control compliance by external service providers on an ongoing basis. 	Selected	Selected	Selected
SA-9 c.e.2	Identification of Functions/ Ports/ Protocols/ Services	The organization requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-10	Developer Configuration Management	<p>The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"> a. Perform configuration management during system, component, or service implementation and operation and maintenance phases of the System Development Life Cycle (SDLC); b. Document, manage, and control the integrity of changes to configuration items identified in the Configuration Management Plan (CMP) c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to the information system or system component NIH and/or IC System Owner, System Administrator, Network Administrator, Data Owner, Business Owner, Project Manager, Services Area Manager and other personnel as appropriate. 	Not Selected	Selected	Selected
SA-11	Developer Security Testing and Evaluation	<p>The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"> a. Create and implement a security assessment plan; b. Perform unit, integration, system, and/or regression testing/evaluation at the level of depth and coverage consistent with NIH and/or IC processes; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation prior to entering the operations and maintenance phase of the SDLC. 	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-12	Supply Chain Protection	<p>The organization protects against supply chain threats to the information system, system component, or information system service by employing risk reviews upon notification of supply chain threats, and wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership), as part of a comprehensive, defense-in-breadth information security strategy.</p> <p><i>Note: Contractors must ensure that these standards of protection are incorporated into the contractor’s property management/control systems. Contractors must also ensure that all of their employees, subcontractors (at all tiers), and employees of each subcontractor who perform work under any HHS, NIH or IC contract/subcontract, comply with these requirements.</i></p>	Not Selected	Not Selected	Selected
SA-15	Development Process, Standards, and Tools	<p>The organization:</p> <ol style="list-style-type: none"> a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: <ol style="list-style-type: none"> 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations at least every three (3) years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy the HHS, NIH, and/or IC documented security requirements. <p><i>Note: Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes.</i></p>	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SA-16	Developer-Provided Training	The organization requires the developer of the information system, system component, or information system service to provide appropriate training (or training materials) on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	Not Selected	Not Selected	Selected
SA-17	Developer Security Architecture and Design	The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: <ul style="list-style-type: none"> a. Is consistent with and supportive of the organization’s security architecture (see PL-8) which is established within and is an integrated part of the organization’s enterprise architecture (see PM-7); b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. 	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.17 Security and Communications Protection (SC)					
SC-1	Systems and Communication Protection Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. System and communication protection policy at least every three (3) years; 2. System and communication protection procedures at least every three (3) years. <p><i>Note: NIH Policy regarding SC-1 is as follows in the remaining SC controls and control enhancements below.</i></p> <p><i>Note: The SC policy and procedures should include a process for modifying traffic management behavior (e.g., re-categorization of uniform resource locators (URLs), modification of category, filtering changes, or granting access to traffic that is blocked by their baseline configuration). This process must address the following: (i) modified access approval by the NIH and/or IC Chief Information Officer (CIO), NIH CISO, or designated authority as appropriate; (ii) a valid and documented business need for modified access; and (iii) technical solutions to define, as narrowly as possible, membership in the access group.</i></p>	Selected	Selected	Selected
SC-2	Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.	Not Selected	Selected	Selected
SC-3	Security Function Isolation	The information system isolates security functions from non-security functions.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SC-4	Information in Shared Resources	The information system prevents unauthorized and unintended information transfer via shared system resources.	Not Selected	Selected	Selected
SC-5	Denial of Service Protection	<p>The information system protects against or limits the effects of the following types of denial of service attacks:</p> <ul style="list-style-type: none"> • Internet Control Message Protocol (ICMP) floods: <ul style="list-style-type: none"> ○ Smurf attack ○ Ping of death ○ Ping flood • Teardrop attack • Peer-to-peer attacks • Permanent DoS attack (i.e., phlashing) • Application level floods: <ul style="list-style-type: none"> ○ Internet Relay Chat (IRC) floods ○ Banana attack ○ Buffer overflow • Nuke • Distributed DoS attack • Reflected attack • Unintentional attack • DoS Level II <p><i>Note: NIH and the ICs refers to the NIST SP 800-61, Computer Security Incident Handling Guide and timely industry information on denial of service attacks to define additional and update existing security safeguards, as required.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SC-7	Boundary Protection	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are in accordance with Assignment 1, 2, or depending on system category and are separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Selected Assignment 1: physically, logically, or both	Selected Assignment 2: physically, logically, or both	Selected Assignment 3: both physically and logically
SC-7 c.e.3	Access Points	The organization limits the number of external network connections to the information system.	Not Selected	Selected	Selected
SC-7 c.e.4	External Telecommunications Services	The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and e. Reviews exceptions to the traffic flow policy at least every 365 days and removes exceptions that are no longer supported by an explicit mission/business need.	Not Selected	Selected	Selected
SC-7 c.e.5	Deny by Default/ Allow by Extension	The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	Not Selected	Selected	Selected
SC-7 c.e.7	Prevent Split Tunneling for Remote Devices	The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SC-7 c.e.8	Route Traffic to Authenticated Proxy Servers	The information system routes NIH approved and defined internal communications traffic to NIH approved and defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices. <i>Note: Proxy servers must support logging of individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and IP addresses and must be configurable with HHS, NIH, and IC lists of authorized and unauthorized websites.</i>	Not Selected	Not Selected	Selected
SC-7 c.e.18	Fail Secure	The information system fails securely in the event of an operational failure of a boundary protection device.	Not Selected	Not Selected	Selected
SC-7 c.e.21	Isolation of Information System Components	The organization employs boundary protection mechanisms to separate information system components supporting critical missions and/or business functions based on a risk analysis.	Not Selected	Not Selected	Selected
SC-8	Transmission Confidentiality and Integrity	The information system protects the confidentiality and integrity of transmitted information. Any transmitted data containing sensitive information, including but not limited to email, must be encrypted using a FIPS 140-2, Security Requirements for Cryptographic Modules compliant encryption solution.	Not Selected	Selected	Selected
SC-8 c.e.1	Cryptographic or Alternate Physical Protection	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by more restrictive HHS, NIH and/or IC safeguards. <i>Note: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003 contains guidance on the use of protective distribution systems, which are physical measures to protect transmitted information.</i>	Not Selected	Selected	Selected
SC-10	Network Disconnect	The information system terminates the network connection associated with a communications session at the end of the session or after 30 minutes or less of inactivity.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SC-12	Cryptographic Key Establishment and Management	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with HHS Standard for Encryption of Computing Devices and Information .	Selected	Selected	Selected
SC-12 c.e.1	Availability	The organization maintains availability of information in the event of the loss of cryptographic keys by users.	Not Selected	Not Selected	Selected
SC-13	Cryptographic Protection	The information system implements cryptographic mechanisms as defined in the HHS Standard for Encryption of Computing Devices and Information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Selected	Selected	Selected
SC-15	Collaborative Computing Devices	The information system: a. Prohibits remote activation of collaborative computing devices with no exceptions ; and b. Provides an explicit indication of use to users physically present at the devices.	Selected	Selected	Selected
SC-17	Public Key Infrastructure Certificates	The organization issues public key certificates under the HHS, NIH or IC certificate policy or obtains public key certificates from an approved service provider. <i>Note: Department-level certificate policy will be forthcoming.</i>	Not Selected	Selected	Selected
SC-18	Mobile Code	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	Not Selected	Selected	Selected
SC-19	Voice Over Internet Protocol	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Selected	Selected	Selected
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. <i>Note: The information system also disables recursive lookups on all publicly accessible domain name system (DNS) servers.</i>	Selected	Selected	Selected
SC-22	Architecture and Provisioning for Name /Address Resolution Service	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Selected	Selected	Selected
SC-23	Session Authenticity	The information system protects the authenticity of communications sessions.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SC-24	Fail in Known State	<p>The information system fails to an NIH or IC System Owner known secure state for all failures preserving the confidentiality, integrity, or availability of system information and failure cause information.</p> <p><i>Note: Failure in a known state can address safety or security in accordance with the mission/business needs of NIH and the ICs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode with less disruption to NIH and IC mission/business processes.</i></p>	Not Selected	Not Selected	Selected
SC-28	Protection of Information at Rest	<p>The information system protects the confidentiality and integrity of NIH and/or IC sensitive data and information at rest to include the state of data and information when it is located on a secondary storage device with an information system.</p> <p><i>Note: Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. NIH and ICs may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.</i></p>	Not Selected	Selected	Selected
SC-39	Process Isolation	<p>The information system maintains a separate execution domain for each executing process.</p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
4.18 System and Information Integrity (SI)					
SI-1	System and Information Integrity Policy and Procedures	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to personnel/roles identified in Appendix A: Roles and Responsibilities of this Handbook: <ul style="list-style-type: none"> 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and, if necessary, updates the current: <ul style="list-style-type: none"> 1. System and information integrity policy at least every three (3) years and 2. System and information integrity procedures at least every three (3) years. <p><i>Note: NIH Policy regarding SI-1 is as follows in the remaining SI controls and control enhancements below.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-2	Flaw Remediation	<p>The organization:</p> <ol style="list-style-type: none"> a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates promptly, in accordance with the note below, of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. <p><i>Note: The timelines to remediate vulnerabilities is designated by the NIH Information Security Program. The following remediation timelines must be met, or the affected device may be removed from the network:</i></p> <ul style="list-style-type: none"> • <i>Critical within 30 days;</i> • <i>High within 60 days;</i> • <i>Medium within 1 year; and</i> • <i>Low within 1 year.</i> 	Selected	Selected	Selected
SI-2 c.e.1	Central Management	The organization centrally manages the flaw remediation process.	Not Selected	Not Selected	Selected
SI-2 c.e.2	Automated Flaw Remediation Status	The organization employs automated mechanisms at least quarterly , to determine the state of information system components with regard to flaw remediation.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-3	Malicious Code Protection	<p>The organization:</p> <ol style="list-style-type: none"> a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: <ol style="list-style-type: none"> 1. Perform periodic scans of the information system at least monthly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Executes one or more of the following in response to malicious code detection: <ul style="list-style-type: none"> • Blocks malicious code • Quarantines malicious code • Sends an alert to the System Administrator; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. <p><i>Note: Malicious code protection can include, for example, anti-virus agents and signature definitions, as well as reputation-based technologies.</i></p>	Selected	Selected	Selected
SI-3 c.e.1	Central Management	The organization centrally manages malicious code protection mechanisms.	Not Selected	Selected	Selected
SI-3 c.e.2	Automatic Updates	The information system automatically updates malicious code protection mechanisms.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-4	Information System Monitoring	<p>The organization:</p> <ul style="list-style-type: none"> a. Monitors the information system to detect: <ul style="list-style-type: none"> 1. Attacks and indicators of potential attacks in accordance with NIH and IC monitoring objectives as described AU-2 and AU-5(2) and 2. Unauthorized local, network, and remote connections (For Moderate and High systems: twice weekly); b. Identifies unauthorized use of the information system through NIH and/or IC techniques and methods as described in AU-6 and AU-7(1); c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides information system monitoring information to NIH Threat Mitigation and Incident Response (TMIR) and System Owners and IC ISSO, System Owners, and security personnel at either an as needed basis and/or, at a minimum, twice weekly for Moderate and High systems. 	Selected	Selected	Selected
SI-4 c.e.2	Automated Tools for Real-Time Analysis	The organization employs automated tools to support near real-time analysis of events.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-4 c.e.4	Inbound and Outbound Communications Traffic	<p>The information system monitors inbound and outbound communications traffic in near real time and continuously for unusual or unauthorized activities or conditions.</p> <p><i>Note: This function may be provided by other entities within the organization, if/when that becomes technically feasible.</i></p>	Not Selected	Selected	Selected
SI-4 c.e.5	System-Generated Alerts	<p>The information system alerts NIH CIO, CISO, TMIR and IC CIO, ISSO, System Owner, and incident response personnel when the following indications of compromise or potential compromise occur:</p> <ul style="list-style-type: none"> • Internal traffic that indicates the presence of malicious code within an information system or propagating among system components • Attack signatures (a characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities) • Signaling to an external information system • Localized, targeted, and network-wide events <p><i>Note: The above list is a minimum set of compromises or potential compromises and may be expanded to include IC-specific items relevant to their missions.</i></p>	Not Selected	Selected	Selected
SI-5	Security Alerts, Advisories, and Directives	<p>The organization:</p> <ol style="list-style-type: none"> a. Receives information system security alerts, advisories, and directives from the United States Computer Emergency Readiness Team (US-CERT) on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to NIH CIO, CISO, TMIR and IC CIO, ISSO, System Owner, and security personnel; and d. Implements security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-5 c.e.1	Security Alerts, Advisories, and Directives	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.	Not Selected	Not Selected	Selected
SI-6	Security Function Verification	<p>The information system:</p> <ol style="list-style-type: none"> Verifies the correct operation of system start-up and restart and at one of the following intervals: <ul style="list-style-type: none"> At defined system transitional states (e.g., system startup, restart). Upon command by a user with appropriate privilege At least every 30 days. Other intervals or functions to meet NIH- or IC-specific needs; Performs this verification upon command by users with the appropriate privileges at the intervals defined in SI-6(a). Notifies the appropriate System Administrators, Network Administrators, and System Owners of failed security verification tests; and Shuts the information system down, restarts the information system, or, performs other NIH- or IC-specific alternative action(s) when anomalies are discovered. 	Not Selected	Not Selected	Selected
SI-7	Software, Firmware, and Information Security	The organization employs integrity verification tools to detect unauthorized changes to NIH and IC software, firmware, data and information .	Not Selected	Selected	Selected
SI-7 c.e.1	Integrity Checks	The information system performs an integrity check of NIH and IC software, firmware, data and information at startup and at least quarterly.	Not Selected	Selected	Selected
SI-7 c.e.2	Automated Notifications of Integrity Violations	The organization employs automated tools that provide notification to NIH CIO, CISO, TMIR and System Owners and IC CIO, ISSO, System Owner, and security personnel upon discovering discrepancies during integrity verification.	Not Selected	Not Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-7 c.e.5	Automated Response to Integrity Violations	The information system automatically executes one or more of the following when integrity violations are discovered: <ul style="list-style-type: none"> • Shuts the information system down. • Restarts the information system. • Implements NIH and/or IC security safeguards. 	Not Selected	Not Selected	Selected
SI-7 c.e.7	Integration of Detection and Response	The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.	Not Selected	Selected	Selected
SI-7 c.e.14	Binary or Machine Executable Code	The organization: <ol style="list-style-type: none"> a. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official. 	Not Selected	Not Selected	Selected
SI-8	Spam Control	The organization: <ol style="list-style-type: none"> a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. 	Not Selected	Selected	Selected
SI-8 c.e.1	Central Management	The organization centrally manages spam protection mechanisms.	Not Selected	Selected	Selected
SI-8 c.e.2	Automatic Updates	The information system automatically updates spam protection mechanisms.	Not Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH InfoSec Program Minimum Requirement by System Category		
			Low	Moderate	High
SI-10	Information Input Validation	<p>The information system checks the validity of information inputs to include, but not limited to:</p> <ul style="list-style-type: none"> All arguments or input data strings submitted by users, external processes, or untrusted internal processes. All values that originate externally to the application program itself, including arguments, environment variables, and information system parameters. Automated data entry transmittal from other servers. <p><i>Note: The information system must trust only reliable external entities which have been identified by authorized NIH and/or IC personnel.</i></p> <p><i>Automated data entry transmittal from other servers must comply with requirements set forth in the procedures found in NIH and IC access controls policies and procedures.</i></p>	Not Selected	Selected	Selected
SI-11	Error Handling	<p>The information system:</p> <ol style="list-style-type: none"> Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and Reveals error messages only to the appropriate Information System Security Officer (ISSO), System Administrators, Network Administrators, and System Owners. 	Not Selected	Selected	Selected
SI-12	Information Handling and Retention	<p>The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.</p>	Selected	Selected	Selected
SI-16	Memory Protection	<p>The information system implements NIH and IC security safeguards such as data execution prevention, address space layout randomization, and other NIH or IC specific safeguards relevant to their security requirements to protect its memory from unauthorized code execution.</p>	Not Selected	Selected	Selected

5 Appendix C: Privacy Controls Section

This section closely follows *National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, Appendix J*, which provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, regardless of format.

Ordinary-font text is derived directly from NIST SP 800-53, Rev 4, while HHS- and NIH-specific assignments are in **green text**. In some cases, controls may have supplemental guidance in the form of an italicized “Note” at the bottom of the Control Description box. Personnel should still consult NIST SP 800-53, Rev 4 Supplemental Guidance sections for more information if needed. Special terms used throughout the Handbook may also be found in the [Glossary](#).

The NIH Office of the Senior Official for Privacy (SOP) collaborated with the NIH Information Security Awareness Office (ISAO), which manages and operates the NIH InfoSec Program, and identified which controls will apply to NIH and ICs. The matrix below contains only the privacy controls selected by NIH SOP. Privacy controls “Not Selected,” “Withdrawn,” or identified as “Not Applicable” are not included in the matrix.

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.1 Authority and Purpose (AP)					
AP-1	Authority to Collect	<p>The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), both generally and in support of specific programs and the needs of information systems.</p> <p><i>Note: PII is information which may be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. PII may pertain to information about any individual, including government employees and members of the public. Truncated social security numbers (SSN), for example, are PII to the same extent as full SSN.</i></p> <p><i>Before collecting PII in a system of records, parties responsible for programs and systems must coordinate with Office of General Counsel through the HHS Senior Agency Official for Privacy (SAOP) and the NIH Senior Official for Privacy (SOP), in order to determine whether the contemplated collection of PII is legally authorized (e.g., by statute or Executive Order) and that there is a link between the authorization and the specific collection of PII. These responsible parties must be able to demonstrate that the collection of PII is necessary to achieve a specifically-authorized goal, purpose or mission.</i></p>	Selected	Selected	Selected
AP-2	Purpose Specification	<p>The organization, at the system or application level, describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy compliance documentation and in its privacy notices (e.g., Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Privacy Act Statements, or Computer Matching Agreements (CMAs)).</p> <p><i>Note: Purpose specification for SSN includes need and reduction/elimination status.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.2 Accountability, Audit, and Risk Management (AR)					
AR-1	Governance and Privacy Program	<p>The organization:</p> <ul style="list-style-type: none"> a. Appoints a Senior Agency Official for Privacy (SAOP) accountable for developing, implementing, and maintaining a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems; <p><i>Note: The HHS SAOP must govern and manage all privacy requirements; however, HHS may appoint other privacy officials and points of contact to support the SAOP so that HHS complies with laws, regulations, and OMB memoranda. These other officials and points of contact may assist with executing items (b)-(f) of this section.</i></p> <ul style="list-style-type: none"> b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates NIH SAOP-defined budget and staffing resources sufficient to implement and operate the organization-wide privacy program; <p><i>Note: NIH SAOP determines the resources required to implement and operate the NIH privacy program in accordance with laws, regulations, and organizational policies for the NIH privacy program.</i></p> <ul style="list-style-type: none"> d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures in accordance with HHS SAOP direction, but at least every two (2) years. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
AR-2	Privacy Impact and Risk Assessment	<p>The organization:</p> <ul style="list-style-type: none"> a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII; and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. <p><i>Note: PIAs for new information systems shall be performed as early in the system development life cycle as possible and prior to collecting, using, maintaining or sharing PII. PIAs are also required whenever an agency uses a third-party website or application (TPWA) to engage openly with the public and make PII available to the agency. PIAs for information systems shall be updated when changes create new privacy risks, when PII is added or deleted from the system, and/or every three (3) years absent a major change.</i></p>	Selected	Selected	Selected
AR-3	Privacy Requirements for Contractors and Service Providers	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; b. Includes privacy requirements in contracts and other acquisition-related documents; and c. Reviews, every two (2) years, a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the contracts include clauses that make all requirements of the Privacy Act apply to the system and that make the criminal penalty provisions of the Privacy Act apply to the contractor or service provider and its personnel. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
AR-4	Privacy Monitoring and Auditing	<p>The organization:</p> <ul style="list-style-type: none"> a. Monitors and audits privacy controls and internal privacy policy at least every 365 days to ensure effective implementation; and b. Documents, tracks, and ensures mitigation of corrective actions identified through monitoring or auditing. <p><i>Note: The HHS SAOP coordinates privacy monitoring and auditing with HHS and NIH information security and privacy officials. Results are provided to senior managers and oversight officials.</i></p>	Selected	Selected	Selected
AR-5	Privacy Awareness and Training ²⁶	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at educating and informing personnel about their privacy responsibilities and procedures; b. Administers basic privacy training at least every 365 days and targeted, role-based privacy training annually for personnel having responsibility for PII or for activities that involve PII at least every 365 days; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least every 365 days. 	Selected	Selected	Selected
AR-6	Privacy Reporting	<p>The organization develops, disseminates, and updates reports to the OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.</p> <p><i>Note: This information will be submitted in response to statutory and regulatory requirements, as appropriate.</i></p>	Selected	Selected	Selected

²⁶ At NIH, new hires must take the NIH Information Security Awareness Course and the NIH Privacy Awareness and Records Management Awareness Course. The annual refresher is a combined course called the Information Security, Counterintelligence, Privacy Awareness, Records Management Refresher.

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
AR-7	Privacy-Enhanced System Design and Development	<p>The organization designs information systems to support privacy by automating privacy controls to the extent feasible, integrating and meeting privacy requirements throughout the EPLC, and incorporating privacy concerns into reviews of significant changes to HHS systems, networks, physical environments, and other agency infrastructures. The organization also conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization’s privacy policy, and any other legal or regulatory requirements.</p> <p><i>Note: The IC conducts periodic reviews of systems to determine if updates are needed due to significant changes in a system's physical environments, infrastructures, networks, or scope.</i></p>	Selected	Selected	Selected
AR-8	Accounting of Disclosures	<p>The organization:</p> <ul style="list-style-type: none"> a. Accounts for authorized and unauthorized disclosures of PII held in each system of records under its control, including: <ul style="list-style-type: none"> 1) Date, nature, and purpose of each disclosure of a record; and 2) Name and address of the person or agency to which the disclosure was made; a. Retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer; and b. Makes the accounting of disclosures available to the person named in the record upon request. <p><i>Note: The term “disclosure” is used in the context of the Privacy Act, and any limitations or exclusions from accounting of disclosures in the Act would also apply.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.3 Data Quality and Integrity (DI)					
DI-1	Data Quality	<p>The organization:</p> <ul style="list-style-type: none"> a. Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems at least every 365 days; and d. Issues guidelines for maximizing the quality, utility, objectivity, and integrity of disseminated information. <p><i>Note: The types of measures implemented to protect data quality must be based on the nature and context of the PII, how it is to be used, and how it was obtained. The measures taken to validate the accuracy of PII must consider whether the PII is used to make determinations about the rights, benefits, or privileges of individuals under federal programs, the sensitivity of the PII, and whether the PII was obtained from sources other than the individual. Parties responsible for programs and systems will assess and identify the frequency with which the data quality must be reviewed and corrected. The assessment must consider legislative or regulatory requirements, the consequences of inaccurate data, and practicable nature of validating the data.</i></p>	Selected	Selected	Selected
DI-1, c.e.1 ²⁷	Validate PII	The organization requests that the individual or individual’s authorized representative validate PII during the collection process.	Selected	Selected	Selected
DI-1, c.e.2	Re-Validate PII	The organization requests that the individual or individual’s authorized representative revalidate that PII collected is still accurate at least every 365 days .	Selected	Selected	Selected

²⁷ c.e. (Control Enhancement). For example, this entry is Control Enhancement 1 (c.e.1).

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.4 Data Minimization and Retention (DM)					
DM-1	Minimization of Personally Identifiable Information	<p>The organization:</p> <ol style="list-style-type: none"> Identifies the minimum PII elements that are relevant and necessary to accomplish the purpose of collection (and where a collection of certain PII requires legal authorization, HHS shall ensure that such collection is legally authorized); Limits the collection and retention of PII to the minimum elements identified in the notice and, when the collection of PII is made directly from the subject individual, limits its purposes to those for which the individual has provided consent to the extent permitted by law; and Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least every 365 days to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish its purpose. <p><i>Note: When periodic evaluations identify opportunities to reduce PII, Plan of Action and Milestone (POA&M) entries must be created for the applicable system or process. NIH must track progress against the POA&M weaknesses until the PII is no longer collected or retained.</i></p> <p><i>Note: HHS and NIH shall use technology to locate and redact PII wherever possible and legally permitted. HHS and NIH shall establish standards for anonymization and de-identification to permit use of the resulting information while reducing its sensitivity and reducing the risks that would result from disclosure. For example, merely redacting the first or last five (5) digits of a Social Security Number (SSN) is neither anonymization nor de-identification.</i></p>	Selected	Selected	Selected
DM-1, c.e.1	Locate/ Remove/ Redact/ Anonymize PII	The organization, where feasible and within the limits of technology and the law, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit authorized use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
DM-2	Data Retention and Disposal	<p>The organization:</p> <ul style="list-style-type: none"> a. Retains each collection of PII for the minimum time period, confirmed by the Records Management Officer to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA) approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses NIH and IC Systems Owners and Privacy Coordinator should follow NIH Policy Manual Chapter 1743, Keeping and Destroying Records, which outlines the approved techniques and/or methods for deleting/destroying PII, to ensure secure deletion or destruction of PII (including originals, copies, and archived records). <p><i>Note: NIH may also use various methods to securely delete or destroy PII, such as those set forth in NIST SP 800-88, Guidelines for Media Sanitization.</i></p>	Selected	Selected	Selected
DM-2, c.e.1	System Configuration	The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a NARA-approved record retention schedule.	Selected	Selected	Selected
DM-3	Minimization of PII Used in Testing, Training, and Research	<p>The organization:</p> <ul style="list-style-type: none"> a. Develops procedures that minimize the use of PII for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research. 	Selected	Selected	Selected
DM-3, c.e.1	Risk Minimization Techniques	The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.5 Individual Participation and Redress (IP)					
IP-1	Consent	<p>The organization:</p> <ul style="list-style-type: none"> a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. <p><i>Note: NIH and ICs should consider the relevant federal, state, and local laws that might apply to their missions and operations.</i></p> <p><i>Note: On HHS, NIH, and IC websites aimed at children under the age of 13, the website must provide mechanisms for parents to provide verifiable consent (and receive appropriate notice) before collecting personal information.</i></p>	Selected	Selected	Selected
IP-1, c.e.1	Mechanisms Supporting Itemized or Tiered Consent	The organization implements mechanisms to support itemized or tiered consent for specific uses of data.	Selected	Selected	Selected
IP-2	Individual Access	<p>The organization:</p> <ul style="list-style-type: none"> a. Provides individuals the ability to have access to their PII maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in SORNs; and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
IP-3	Redress	<p>The organization:</p> <ul style="list-style-type: none"> a. Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. 	Selected	Selected	Selected
IP-4	Complaint Management	<p>The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.</p> <p><i>Note: The organization provides complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the SAOP or other official designated to receive complaints), and are easy to use. Complaint management processes include tracking mechanisms for complaint receipt, review, and disposition.</i></p>	Selected	Selected	Selected
IP-4, c.e.1	Response Times	<p>The organization:</p> <ul style="list-style-type: none"> a. Acknowledges complaints, concerns, or questions from individuals within 10 working days; b. Completes review of requests within 30 working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time; and c. Responds to any appeal as soon as possible, but no later than 30 working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period. 	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.6 Security (SE)					
SE-1	Inventory of Personally Identifiable Information	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes, maintains, and updates at least every 365 days an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and b. Provides each update of the PII inventory to the CIO or information security official at least every 365 days to support the establishment of information security requirements for all new or modified information systems containing PII. <p><i>Note: The PII inventory identifies: (i) the name and acronym for each program and system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII as collected, used, maintained, or shared by that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed.</i></p> <p><i>The NIH OSOP and ISAO provide reports to HHS outlining PII inventory at least every 365 days.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
SE-2	Privacy Incident Response	<p>The organization:</p> <ol style="list-style-type: none"> a. Develops and implements a Privacy Incident Response Plan²⁸; and b. Provides an organized and effective response to privacy incidents in accordance with the HHS Privacy Incident Response Plan. <p><i>Note: The NIH and the ICs' Privacy Incident Response Plans must support an internal reporting process that complies with the HHS Privacy Incident Response Plan, and includes:</i></p> <ul style="list-style-type: none"> • <i>The establishment of a cross-functional team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan;</i> • <i>A process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly;</i> • <i>A privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks;</i> • <i>Internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the HHS SAOP, consistent with organizational incident management structures; and</i> • <i>Internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials.</i> 	Selected	Selected	Selected

²⁸ At NIH, the NIH Policy Manual Chapter 1745-2, Privacy and Information Security Incident and Breach Response Policy, is the Privacy Incident Response Plan.

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.7 Transparency (TR)					
TR-1	Privacy Notice	<p>The organization:</p> <ul style="list-style-type: none"> a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to request access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes (such as the use or collection of information by the website or system) in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change. <p><i>Note: Notice includes identifying on public websites the web measurement and customization technologies in use on the websites. The web measurement and customization technologies must be consistent with OMB Memorandum 10-22 and HHS standards operating procedures. Prior to notification of and use of Tier-3 web management and customization technologies, the NIH receives HHS SAOP approval for the use. Also, prior to notification of and use of Tier 3 web measurement and customization technologies, HHS and NIH solicit feedback from the public and adjudicate issues as appropriate.</i></p>	Selected	Selected	Selected
TR-1, c.e.1	Real-Time or Layered Notice	The organization provides real-time and/or layered notice when it collects PII.	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
TR-2	System of Records Notices and Privacy Act Statements	<p>The organization, through the HHS Privacy Act Officer, NIH SOP, NIH Privacy Coordinators/Contacts, and the HHS Office of General Counsel:</p> <ul style="list-style-type: none"> a. Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII; b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. <p><i>Note: NIH and ICs may also consult with other privacy or program stakeholders, as needed, if that interaction would enhance privacy protections for the public or would assist in understanding business requirements.</i></p> <p><i>The NIH OSOP reviews IC submitted SORNs for accuracy and completeness. Then works with HHS during the OMB oversight process. Finalizing in the publishing of SORNs in the Federal Register.</i></p>	Selected	Selected	Selected
TR-2, c.e.1	Public Website Publication	<p>The organization publishes SORNs on its public website.</p> <p><i>Note: The NIH OSOP maintains a current link to HHS' SORN website where published SORNs can be found and read.</i></p>	Selected	Selected	Selected
TR-3	Dissemination of Privacy Program Information	<p>The organization:</p> <ul style="list-style-type: none"> a. Ensures that the public has access to information about its privacy activities and is able to communicate with its HHS SAOP/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise. <p><i>Note: HHS, NIH, ICs must disclose publicly the use of third-party websites and applications (TPWAs) and web measurement and customization technologies used on HHS, NIH, and ICs' websites.</i></p>	Selected	Selected	Selected

Control ID	Control Title	Control Description	NIH SOP Minimum Requirement by System Category		
			Low	Moderate	High
5.8 Use Limitation (UL)					
UL-1	Internal Use	The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	Selected	Selected	Selected
UL-2	Information Sharing with Third Parties	<p>The organization:</p> <ul style="list-style-type: none"> a. Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required; <p><i>Note: The HHS SAOP (in coordination with the NIH SOP) and legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s).</i></p>	Selected	Selected	Selected

6 Appendix D: Acronyms List

The following matrix contains a list of acronyms that may be in use across NIH. Some of the acronyms below may not be in this document, however, are provided to ensure the acronyms are expanded consistently across the enterprise.

Acronym	Full Term
Δ	Delta
A&A	Assessment and Authorization
ABAC	Attribute Based Access Control
AC	Access Control
AD	Active Directory
AF	Alternate Facility
AMS	Access Management Services
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ARF	Asset Reporting Format
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
AV	Antivirus
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BIOS	Basic Input Output System
BLSR	Baseline Security Requirements
BPA	Blanket Purchase Agreement
BRM	Business Reference Model
BY	Budget Year
C&A	Certification and Accreditation
CA	Certificate Authority/Certificate Authorities
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCB	Configuration/Change Control Board
CCE	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIPS	Computer Crime and Intellectual Property Section
CCRB	Configuration Control Review Board
CCSS	Common Configuration Scoring System
CD	Compact Disk
CDM	Continuous Diagnostics Mitigation
CD-R	Compact Disk-Recordable
CEE	Common Event Expressions
CERIAS	Center for Education and Research in Information Assurance and Security
CERT/CC	CERT Coordination Center

Acronym	Full Term
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CFR	Code of Federal Regulations
CI	Configuration Item
CIKR	Critical Infrastructure And Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPSE	Confidential Information Protection and Statistical Efficiency Act
CIRC	Computer Incident Response Capability
CIRC	Computer Incident Response Center
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CIT	Center for Information Technology
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CMS	Credential Management Services
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations
COPPA	Children's Online Privacy Protection Act
COTS	Commercial Off-The-Shelf
CP	Contingency Plan/Contingency Planning
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CSF	Cybersecurity Framework
CSIRC	Computer Security Incident Response Capability
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSR	Center for Scientific Review
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CY	Current Year
DAA	Designated Approving Authority
DASD	Direct Access Storage Device
DB	Database
DBA	Database Administrator
DCS	Distributed Control System
DDoS	Distributed Denial of Service

Acronym	Full Term
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoD	Department of Defense
DoS	Denial of Service
DRM	Data and Information Reference Model
DRP	Disaster Recovery Plan
DS	Digital Signal
DVD	Digital Video Disc
DVD-R	Digital Video Disk-Recordable
DVD-ROM	Digital Video Disc - Read-Only Memory
DVD-RW	Digital Video Disc - Rewritable
EA	Enterprise Architecture
EAP	Employee Assistance Program
E-Auth	E-Authentication
EFS	External File Sharing
eGRC	Enterprise Governance Risk and Compliance
EMP	Electromagnetic Pulse
EMSEC	Emissions Security
EO	Executive Officer
EPLC	Enterprise Performance Life Cycle
EPP	Endpoint Protection Platform
ERA	E-Authentication Risk Assessment
ETA	E-Authentication Threshold Analysis
FAM	Financial Audit Manual
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FCD	Federal Continuity Directive
FDCC	Federal Desktop Core Configuration
FEA	Federal Enterprise Architecture
FEA SPP	Federal Enterprise Architecture Security and Privacy Profile
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FFMIA	Federal Financial Management Improvement Act
FIC	Fogarty International Center
FICAM	Federal Identity, Credential, and Access Management
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FIS	CIT Facility and Infrastructure Services
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act

Acronym	Full Term
FITSAF	Federal Information Technology Security Assessment Framework
FMFIA	Federal Managers Financial Integrity Act
FOIA	Freedom of Information Act
FPC	Federal Preparedness Circular
FS	Federation Services
FTE	Full-Time Equivalent
GAO	Government Accountability Office
GB	Gigabyte
GFIRST	Government Forum of Incident Response and Security Teams
GLB	Gramm-Leach-Bliley Act
GOTS	Government Off-the-Shelf
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GRC	Governance Risk and Compliance
GRS	General Record Schedule
GSA	General Services Administration
GSS	General Support System
HA	High Availability
HEW U.S.	Department of Health, Education, and Welfare
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVA	High Value Asset
HVAC	Heating, Ventilation, And Air Conditioning
HW	Hardware
I/O	Input/Output
IA	Information Assurance
IaaS	Infrastructure as a Service
IAM	Identity, Credential, and Assess Management Services
IANA	Internet Assigned Numbers Authority
IC	Institutes and Centers
ICS	Industrial Control System
ID	Identification
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IG	Inspector General
IIF	Information in Identifiable Form
IIHI	Individually Identifiable Health Information

Acronym	Full Term
IMS	Identity Management Services
InfoSec	NIH Information Security Program
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPA	Initial Privacy Assessment
IPSec	Internet Protocol Security
IR	Incident Response
IR	Interagency Report
IRB	Investment Review Board
IRC	Internet Relay Chat
IS	Information System
ISA	Interconnection Security Agreement
ISAC	Information Sharing and Analysis Center
ISC	Information System Component
ISC²	International Information Systems Security Certification Consortium
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISD	Instructional System Methodology
ISDN	Integrated Services Digital Network
ISO	Information System Owner or International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
ISP	Internet Service Provider
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISU	Information System User
IT	Information Technology
ITCP	Information Technology Contingency Plan
ITIL	Information Technology Infrastructure Library
ITL	Information Technology Laboratory
KSA	Knowledge, Skills, and Abilities
LACS	Logical Access Control System
LAN	Local Area Network
LCC	Life Cycle Cost
LDAP	Lightweight Directory Access Protocol
LSI	Large-Scale Integration
MA	Major Application
MAC	Media Access Control
MAO	Maximum Allowable Outage
MB	Megabyte
Mbps	Megabits Per Second
MEF	Mission Essential Functions

Acronym	Full Term
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSEL	Master Scenario Events List
MSSP	Managed Security Services Provider
MTD	Maximum Tolerable Downtime
MTTF	Mean Time To Failure
NARA	National Archives and Records Administration
NAS	Network-Attached Storage
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NC	Non-component
NCATS	National Center for Advancing Translational Sciences
NCCIC	National Cybersecurity and Communications Integration Center
NCCIH	National Center for Complementary and Integrative Health
NCI	National Cancer Institute
NDA	Non-Disclosure Agreement
NEF	National Essential Functions
NEI	National Eye Institute
NetBIOS	Network Basic Input/Output System
NFO	Nonfederal Organization
NHGRI	National Human Genome Research Institute
NHLBI	National Heart, Lung, and Blood Institute
NIA	National Institute on Aging
NIAAA	National Institute on Alcohol Abuse and Alcoholism
NIAD	National Institute of Allergy and Infectious Diseases
NIAMS	National Institute of Arthritis and Musculoskeletal and Skin Diseases
NIAP	National Information Assurance Partnership
NIBIB	National Institute of Biomedical Imaging and Bioengineering
NICHD	National Institute of Child Health and Human Development
NIDA	National Institute on Drug Abuse
NIDCD	National Institute on Deafness and Other Communication Disorders
NIDCR	National Institute of Dental and Craniofacial Research
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIEHS	National Institute of Environmental Health Sciences
NIGMS	National Institute of General Medical Sciences
NIH	National Institutes of Health
NIH CC	NIH Clinical Center
NIMH	National Institute of Mental Health
NIMHD	National Institute on Minority Health and Health Disparities
NINDS	National Institute of Neurological Disorders and Stroke
NINR	National Institute of Nursing Research
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report

Acronym	Full Term
NKS	NIH Key Systems
NLM	National Library of Medicine
NOFORN	Not Releasable to Foreign Nationals
NPPI	Non-Public Personal Information
NSA	National Security Agency
NSAT	NIH Security Authorization Tool
NSP	Network Service Provider
NSPD	National Security Presidential Directive
NSRL	National Software Reference Library
NSTISSI	National Security Telecommunications and Information System Security Instruction
NTP	Network Time Protocol
NVD	National Vulnerability Database
NVD	National Vulnerability Database (formerly known as I-CAT)
OCI	Organizational Conflict of Interest
OCIL	Open Checklist Interactive Language
OCIO	Office of the Chief Information Officer
OD	NIH Office of the Director
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OEP	Occupant Emergency Plan
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OpDivs	Operating Divisions
OPM	Office of Personnel Management
OPSEC	Operations Security
ORS	Office of Research Services
OS	Operating System
OSOP	NIH Office of the Senior Official for Privacy
OT	Operations Technology
OVAL	Open Vulnerability and Assessment Language
P2P	Peer-to-Peer
PaaS	Platform as a Service
PACS	Physical Access Control System
PBX	Private Branch Exchange
PCIE	President's Council on Integrity and Efficiency
PDA	Personal Digital Assistant
PHI	Protected Health Information
PI	Pandemic Influenza
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identification Verification Interoperable
PKI	Public Key Infrastructure

Acronym	Full Term
PL	Public Law
PMA	President's Management Agenda
PMEF	Primary Mission Essential Functions
PMP	Project Management Professional
POA&M or POA&Ms	Plan of Action and Milestones
POC	Point of Contact
PRA	Paperwork Reduction Act
PRISMA	Program Review for Information Security Management Assistance
PRM	Performance Reference Model
PTA	Privacy Threshold Analysis
PY	Prior Year
RAID	Redundant Array Of Independent Disks
RAR	Risk Assessment Report
RBAC	Role-Based Access Control
RD	Restricted Data
REN-ISAC	Research and Education Networking Information Sharing and Analysis Center
Rev.	Revision
RFC	Request for Comment
RFID	Radio-Frequency Identification
RID	Real-Time Inter-Network Defense
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA&A	Security Assessment & Authorization
SaaS	Software as a Service
SAISO	Senior Agency Information Security Officer
SAMI	Sources And Methods Information
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network, Security
SAOP	Senior Agency Official for Privacy
SAP	Security Assessment Plan or Special Access Program
SAR	Security Assessment Report
SC	Security Category
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCF	Security Control Families
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SecCM	Security-Focused Configuration Management
SIA	Security Impact Analysis
SIEM	Security Information and Event Management

Acronym	Full Term
SISO	Senior Information Security Officer
SLA	Service-Level Agreement
SOA	Service-Oriented Architecture
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SOR	System of Records
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication
SPP	Security and Privacy Profile
SRM	Service Component Reference Model
SSE	Systems Security Engineering - Capability Maturity Model®
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Social Security Number
SSP	System Security Plan
ST&E	Security, Test, and Evaluation
StaffDivs	Staff Divisions
STIG	Security Technical Implementation Guidelines
SW	Software
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TERENA	Trans-European Research and Education Networking Association
TMIR	Threat Mitigation and Incident Response
TRM	Technical Reference Model
TT&E	Test, Training, and Exercise
U.S.	United States
U.S.C.	United States Code
UDP	User Datagram Protocol
UII	Unique Item Identifier
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team ³⁴
USGCB	United States Government Configuration Baseline
UTC	Coordinated Universal Time
UTSA	University of Texas-San Antonio
VLAN	Virtual Local Area Network
VM	Virtual Machine/Vulnerability Management
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTL	Virtual Tape Library
WAN	Wide Area Network

Acronym	Full Term
WiFi or Wi-Fi	Trademarked phrase (common name) for IEEE 802.11x
WLAN	Wireless Local Area Network
WORM	Write-Once, Read-Many
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

7 Appendix E: Glossary

The following matrix contains a list of InfoSec terms that may be in use across NIH. Some of the terms below may not be in this document, however, the terms are provided to ensure the terms are defined consistently across the enterprise.

InfoSec Term	Definition
Δ (Delta)	Delta's most common meaning is that of difference or change in something. For example, the change information from the last report based on the reporting frequency. (Derived from Study.com, <i>What is Delta? – Definition & Concept</i>)
Access Control (AC)	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Active Directory (AD)	Active Directory (AD) is a Microsoft technology used to manage computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers. (Defined in the <i>Tech Terms Computer Dictionary</i>)
Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Adequate Security	Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Advanced Persistent Threat (APT)	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. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)

InfoSec Term	Definition
Agency	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. (Defined in FIPS 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i>)
Allocation	The process an organization employs to assign controls to specific information system components responsible for providing a security or privacy capability (e.g., router, server, remote sensor). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Analysis Approach	The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Application	A software program hosted by an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assessment Approach	The approach used to assess risk and its contributing risk factors, including quantitatively, qualitatively, or semi-quantitatively. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assessment Findings	Assessment results produced by the application of an assessment procedure to a security control, privacy control, or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assessment Method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assessment Object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assessment Objective	A set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assessment Procedure	A set of assessment objectives and an associated set of assessment methods and assessment objects. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Assurance Case	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Audit Record	An individual entry in an audit log related to an audited event. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Audit Reduction Tools	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (Defined in FIPS 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i>)
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>) (*2 nd Part of Assessment and Authorization A&A Process)
Authorization to Operate (ATO)	The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)

InfoSec Term	Definition
Authorizing Official (AO)	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Authorizing Official Designated Representative (AODR)	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization or privacy authorization. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Availability	Ensuring timely and reliable access to and use of information. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Baseline	Hardware, software, databases, and relevant documentation for an information system at a given point in time. (Defined in NIST SP 800-161, <i>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i> and NISTIR 7622, <i>Notional Supply Chain Risk Management Practices for Federal Information Systems</i>)
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Baselining	Monitoring resources to determine typical utilization patterns so that significant deviation can be detected. (Defined in NIST SP 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Basic Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Blacklisting	The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited Universal Resource Locators (URL)/websites. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Business Areas	“Business areas” separate government operations into high-level categories relating to the purpose of government, the mechanisms the government uses to achieve its purposes, the support functions necessary to conduct government operations, and resource management functions that support all areas of the government’s business. “Business areas” are subdivided into “areas of operation” or “lines of business.” The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Central Management	The organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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 the system. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Change/Configuration Control Board (CCB)	A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system. (Defined in <i>CNSSI-4009</i>)
Chief Financial Officer (CFO)	The CFO is the senior financial advisor to the investment review board (IRB) and the agency head. Information security investments fall within the purview of the CFO and are included in the CFO’s reports. (Defined in <i>NIST SP 800-100, Information Security Handbook: A Guide For Managers</i>)

InfoSec Term	Definition
Chief Information Officer (CIO)	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired, and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Chief Information Security Officer (CISO)	Official responsible for carrying out the chief information officer (CIO) responsibilities under the Federal Information Security Management Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. Note: Also known as senior information security officer (SISO) or chief information security officer (CISO). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Chief Privacy Officer(CPO)	The senior organizational official with overall organization-wide responsibility for information privacy issues. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Chief Security Officer (CSO)	Manages an organization's security and is the ultimate manager and custodian of an enterprise's data, infrastructure, and entire physical and digital assets. CSO also plans and implements an organization's security policy, architecture, and framework. (Defined at <i>Technopedia</i>)
Classified National Security Information	Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Cloud Computing	Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. (Defined in NIST SP 800-145, <i>The NIST Definition of Cloud Computing</i>)

InfoSec Term	Definition
Command and Control	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Commercial Off-the-Shelf (COTS)	Technology and/or a product that is ready-made and available for sale, lease, or license to the general public. (Defined in NIST SP 800-130, <i>A Framework for Designing Cryptographic Key Management Systems</i>)
Commodity Service	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Common Carrier	In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Common Control	A security control that is inheritable by one or more organizational information systems. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Common Control Provider	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inheritable by information systems). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Common Criteria	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Common Secure Configuration	A recognized standardized and established benchmark that stipulates specific secure configuration settings for a given information technology platform.
Compensating Security Controls	The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Computer Matching Agreement	An agreement entered into by an organization in connection with a computer matching program to which the organization is a party, as required by the Computer Matching and Privacy Protection Act of 1988. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Computer Security Incident	See “Incident.”
Computer Security Incident Response Team (CSIRT)	A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Configuration Control	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Configuration Item (CI)	An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Configuration Management (CM)	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Contingency Plan (CP)	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. (Defined in NIST SP 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>)
Continuity of Operations (COOP) Plan	A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. (Defined in <i>NIST SP 80-34 Rev 1: Contingency Planning Guide for Federal Information Systems</i>)
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Controlled Area	Any area or space for which an organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Controlled Interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Controlled Unclassified Information (CUI)	Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. (Defined in the <i>Federal Register 32 CFR Part 2002: Controlled Unclassified Information; Final Rule</i>)
Counterintelligence	Information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. (Defined in FIPS 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i>)
Course of Action	A time-phased or situation-dependent combination of risk response measures. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Covert Channel Analysis	Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Covert Storage Channel	Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Covert Timing Channel	Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Critical Infrastructure Sectors	Information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. (Defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Cross Domain Solution	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Cryptographic Module Validation Program (CMVP)	The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada that validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or designated information (Canada). (Defined in FIPS 140-2, <i>Security Requirements for Cryptographic Modules</i>)
Cryptologic	Of or pertaining to cryptology. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)

InfoSec Term	Definition
Cryptology	The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Cybersecurity Framework (CSF)	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. (Defined in <i>NIST Framework for Improving Critical Infrastructure Cybersecurity</i>).
Cyberspace	The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Data Mining/Harvesting	An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Defense-in-Breadth	A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Defense-in-Depth	Information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Developer	A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Discretionary Access Control	<p>An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability.</p> <p>A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)</p>
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Dynamic Subsystem	A subsystem that is not continually present during the execution phase of an information system. Service-oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
e-Authentication (e-Auth) Assurance Level	A measure of trust or confidence in an authentication mechanism defined in OMB Memorandum M-04-04 and SP 800-63, in terms of four levels: • Level 1: LITTLE OR NO confidence • Level 2: SOME confidence • Level 3: HIGH confidence • Level 4: VERY HIGH confidence. (Defined in <i>FIPS 201-2</i>) (*Risk Assessments are conducted to determine e-Auth Assurance Level)

InfoSec Term	Definition
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Enterprise Architecture (EA)	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Enterprise Performance Lifecycle (EPLC)	A framework that establishes a project management and accountability environment where HHS information technology projects achieve consistently successful outcomes that maximize alignment with HHS-wide and individual NIH goals and objectives. Implementation of the EPLC methodology allows HHS to improve the quality of project planning and execution, reducing overall project risk. (Defined in HHS-OCIO-2008-0004.001, <i>HHS OCIO Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC)</i>)
Environment of Operation	The physical, technical, and organizational setting in which an information system operates, including but not limited to: missions/business functions; mission/business processes; threat space; vulnerabilities; enterprise and information security architectures; personnel; facilities; supply chain relationships; information technologies; organizational governance and culture; acquisition and procurement processes; organizational policies and procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs). (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Event	Any observable occurrence in a network or system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i> and NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control or privacy control effectiveness over time. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Executive Agency	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. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
Exfiltration	The unauthorized transfer of information from an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
External Network	A network not controlled by the organization. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Fair Information Practice Principles	Principles that are widely accepted in the United States and internationally as a general framework for privacy and that are reflected in various federal and international laws and policies. In a number of organizations, the principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
False Positive	An alert that incorrectly indicates that malicious activity is occurring. Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Fault Tree Analysis	A top-down, deductive failure analysis in which an undesired state of a system (top event) is analyzed using Boolean logic to combine a series of lower-level events. An analytical approach whereby an undesired state of a system is specified, and the system is then analyzed in the context of its environment of operation to find all realistic ways in which the undesired event (top event) can occur. (As defined in NIST SP 800-30, Rev.1, <i>Guide for Conducting Risk Assessments</i>)

InfoSec Term	Definition
Federal Enterprise Architecture (FEA)	A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Federal Information System	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. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Federal Risk and Authorization Management Program (FedRAMP)	A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. (Defined on the <i>U.S. General Service Administration (GSA) Website</i>)
Federal Security and Management Act (FISMA)	Requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget (OMB). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
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). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Firmware	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
General Support System (GSS)	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Government Information	Information created, collected, processed, disseminated, or disposed of by or for the Federal Government. (NIH ISAO Governance, Risk, and Compliance)

InfoSec Term	Definition
Government Off-the-Shelf (GOTS)	A software and/or hardware product that is developed by the technical staff of a Government organization for use by the U.S. Government. GOTS software and hardware may be developed by an external entity, with specification from the Government organization to meet a specific Government purpose and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the Government. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Guard (System)	A mechanism limiting the exchange of information between information systems or subsystems. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Hardware	The physical components of an information system. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Health Insurance Portability and Accountability Act (HIPAA) of 1996	HIPAA required the Secretary to adopt, among other standards, security standards for certain health information. These standards, known as the HIPAA Security Rule (the Security Rule), were published on February 20, 2003. (Defined in <i>NIST SP 800-66, Rev 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule</i>)
High Value Asset (HVA)	High Value Assets (HVA) are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. (Defined in OMB Memorandum M-17-09, <i>Management of Federal High Value Assets</i>)
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See Common Control and System-Specific Security Control. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Impact Level	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Impact Value	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Incident Handling	The mitigation of violations of security policies and recommended practices. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Incident Response (IR)	See “Incident Handling.”
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s information systems(s). (Defined in NIST SP 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>)
Independent Assessor	Any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. (Defined in NIST SP 800-37, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i>)
Independent Regulatory Agency	The Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Indicator	A sign that an incident may have occurred or may be currently occurring. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Individual	A citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Industrial Control System (ICS)	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information	Facts and ideas, which can be represented (encoded) as various forms of data. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Information Leakage	The intentional or unintentional release of information to an untrusted environment. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information Owner/Steward	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Information Security Architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. (Defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Information Steward	Individual or group that helps to ensure the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of the Federal Information Security Management Act (FISMA) and any associated security-related federal policies, directives, regulations, standards, and guidance. (Defined in NIST SP 800-37 Rev.1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach</i>)
Information System (IS)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Information System Component (ISC)	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information System Owner (ISO)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information System Resilience	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Information System Security Engineer (ISSE)	Individual assigned responsibility for conducting information system security engineering activities. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Information System Security Officer (ISSO)	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Information System-related Security Risks	Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Information Technology Contingency Plan (ITCP)	Interim measures to recover IT services following an emergency or system disruption. (Defined in NIST SP 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>)
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (Defined in <i>NIST SP 800-145: The NIST Definition of Cloud Computing</i>)
Institute of Electrical and Electronics Engineers (IEEE)	The Institute of Electrical and Electronics Engineers is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. (Defined in <i>IEEE Mission & Vision Statement</i>)
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)

InfoSec Term	Definition
Intelligence	Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Intelligence Activities	The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Intelligence Community (IC)	The term 'intelligence community' refers to the following agencies or organizations: (i) The Central Intelligence Agency (CIA); (ii) The National Security Agency (NSA); (iii) The Defense Intelligence Agency (DIA); (iv) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; (v) The Bureau of Intelligence and Research of the Department of State; (vi) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and (vii) The staff elements of the Director of Central Intelligence. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Interconnection Service Agreement (ISA)	An agreement established between the organizations that own and operate connected information systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. (Defined in NIST SP 800-47, <i>Security Guide for Interconnecting Information Technology Systems</i>)
Interface	Common boundary between independent systems or modules where interactions take place. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control and privacy control effectiveness over time. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Intrusion Detection and Prevention System (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Joint Authorization	Security authorization involving multiple authorizing officials. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., Initialization Vectors and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. (Defined in NIST SP 800-57, <i>Recommendation for Key Management</i>)
Key Recovery	A function in the life cycle of keying material; mechanisms and processes that allow authorized entities to retrieve keying material from key backup or archive. (Defined in NIST SP 800-57, <i>Recommendation for Key Management</i>)
Likelihood of Occurrence	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. (<i>SP 800-30 Rev.1 Guide for Conducting Risk Assessments</i>)
Lines of Business	“Lines of business” or “areas of operation” describe the purpose of government in functional terms or describe the support functions that the government must conduct in order to effectively deliver services to citizens. Lines of business relating to the purpose of government and the mechanisms the government uses to achieve its purposes tend to be mission-based. Lines of business relating to support functions and resource management functions that are necessary to conduct government operations tend to be common to most agencies. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Local Access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Local Area Network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. (Defined in <i>NIST SP 800-82 Rev 2: Guide to Industrial Control Systems</i>)
Logical Access Control System	An automated system that controls an individual’s ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual’s identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)

InfoSec Term	Definition
Major Application (MA)	<p>An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.</p> <p>Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Malicious Code	<p>Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Malware	<p>A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)</p>
Managed Interface	<p>An interface within an information system that provides boundary protection capability using automated mechanisms or devices. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Management Controls	<p>The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (Defined in NIST SP 800-37 Rev.1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Lifestyle Approach</i>)</p>
Mandatory Access Control	<p>An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)</p>
Mechanisms	<p>An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>

InfoSec Term	Definition
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Media Access Control (MAC)	A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer. (Defined in <i>NIST SP 800-121 Rev 1: Guide to Bluetooth Security</i>)
Memorandum of Understanding/Agreement (MOU/A)	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (Defined in NIST SP 800-47, <i>Security Guide for Interconnecting Information Technology Systems</i>)
Minor Application	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Mission Critical	Any telecommunications or information system that is defined as a national security system (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Mission Essential Functions (MEF)	Mission essential functions (MEFs) are the limited set of department and agency level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal operations. (Derived from U.S. Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 1, <i>Federal Executive Branch National Continuity Program and Requirements</i>)
Mission/Business Segment	Elements of organizations describing mission areas, common/shared business services, and organization-wide services. Mission/business segments can be identified with one or more information systems which collectively support a mission/business process. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Mobile Device	<p>A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.</p> <p>Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high. (Defined in NIST SP 800-18, <i>Guide for Developing Security Plans for Federal Information Systems</i>)
Multifactor Authentication (MFA)	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Multilevel Security	Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Multiple Security Levels (MSL)	Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
<p>National Essential Functions (NEF)</p>	<p>NEFs are MEFs that shall be the primary focus of the Federal Government leadership during and in the aftermath of an emergency that adversely affects the performance of government and include the following:</p> <ul style="list-style-type: none"> a. Ensuring the continued functioning of our form of government under the Constitution, including the functioning of three separate branches of government; b. Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people; c. Defending the Constitution of the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interests; d. Maintaining and fostering effective relationships with foreign nations; e. Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests; f. Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident; g. Protecting and stabilizing the Nation’s economy and ensuring public confidence in its financial systems; and h. Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States <p>(Derived from U.S. Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 1, <i>Federal Executive Branch National Continuity Program and Requirements</i>)</p>
<p>National Security Emergency Preparedness Telecommunications Services</p>	<p>Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
<p>National Security Information (NSI)</p>	<p>Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)</p>

InfoSec Term	Definition
National Security System (NSS)	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
National Vulnerability Database (NVD)	The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics. (Defined at https://nvd.nist.gov/)
Net-centric Architecture	A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service-oriented architectures and cloud computing architectures. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Network Access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
NIH Security Authorization Tool (NSAT)	<p>NSAT is an Assessment & Authorization (A&A) tool that allows NIH to assess Federal Information Security Management Act (FISMA), Privacy Act, and Office of Management and Budget (OMB) Circular A-130 (OMB A-130) compliance and authorize information systems across the NIH enterprise to ensure these systems are operating at an acceptable level of risk. It provides NIH, and its Institutes and Centers (ICs), with the capability to define authorization boundaries, allocate and assess security and privacy controls, assemble authorization packages, make informed authorization decisions, and determine whether each information system stays within acceptable risk parameters.</p> <p>Specifically, NSAT allows NIH and the ICs to:</p> <ul style="list-style-type: none"> • Centrally manage procedures and security and privacy controls • Catalog business and technical hierarchies for compliance reporting • Build an integrated security and privacy controls framework through policies and standards • Map security and privacy controls to key business elements, system components, and compliance evidence • Manage the policy and security and privacy controls compliance lifecycle • Clearly establish and justify security categorizations • Customized security and privacy control allocation and assessment • Manage and track weaknesses and remediation (POA&M) • Monitor compliance strategy and Ongoing Authorization (OA) <p>(Defined in <i>NIH InfoSec Program System Security Plan (SSP)</i>)</p>
Nonlocal Maintenance	<p>Maintenance activities conducted by individuals communicating through a network, either an external network or internal network. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Non-Organizational User	<p>A user who is not an organizational user (including public users). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Non-repudiation	<p>Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
NSA-Approved Cryptography	<p>Cryptography that consists of an approved algorithm; an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a specific environment; and a supporting key management infrastructure. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)</p>
Object	<p>Passive system-related entity including, for example, devices, files, records, tables, processes, programs, and domains, that contain or receive information. Access to an object (by a subject) implies access to the information it contains. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)</p>

InfoSec Term	Definition
Ongoing Assessment	The continuous evaluation of the effectiveness of security control or privacy control implementation; with respect to security controls, a subset of Information Security Continuous Monitoring (ISCM) activities. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Operations Security (OPSEC)	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Organizational User	An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Overlay	A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Patch	An additional piece of code developed to address a problem in an existing piece of software. (Defined in NIST SP 800-40 Version 2.0, <i>Creating a Patch and Vulnerability Management Program</i>)
Peer-to-Peer (P2P)	Any software or system allowing individual users of the Internet to connect to each other and trade files. (Defined in OMB M-04-26, Personal Use Policies and 'File Sharing' Technologies)
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Personal Identity Verification (PIV)	A physical artifact (e.g., identity card, “smart” card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in FIPS PUB 201. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Physical Access Control System (PACS)	An electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points. (Defined in NIST SP 800-116 <i>Guidelines for the Use of PIV Credentials in Facility Access</i>)
Plan of Action and Milestones (POAM, POA&M or POA&Ms)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. ³ The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (Defined in NIST SP 800-145: <i>The NIST Definition of Cloud Computing</i>)
Policy	The rules and regulations set by an organization that define the purpose of the program and its scope within an organization; assigns responsibilities for direct program implementation, as well as other responsibilities to related offices (e.g., Chief Information Office); and addresses compliance issues. A program policy sets organizational and strategic directions for security and assigns resources for the program’s implementation. (Defined in NIST SP 800-12, <i>An Introduction to Information Security</i>)
Portable Media	Any device that can store data electronically and is portable, such as portable hard drives, universal serial bus (USB) drives, secure digital (SD) card media, compact discs – read only memory (CD-ROMs), and digital video discs (DVDs). (Defined in the <i>HHS Standard for Encryption of Computing Devices and Information</i>)

InfoSec Term	Definition
Portable Storage Device	<p>Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. Note: Examples include, but are not limited to: USB flash drives, external hard drives, and external solid-state disk (SSD) drives. Portable Storage Devices also include memory cards that have additional functions aside from standard data storage and encrypted data storage, such as built-in Wi-Fi connectivity and global positioning system (GPS) reception. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Potential Impact	<p>The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)</p>
Precursor	<p>A sign that an attacker may be preparing to cause an incident. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)</p>
Predisposing Condition	<p>A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation. (Defined in NIST SP 800-82 Rev.2, <i>Guide to Industrial Control Systems (ICS) Security</i>)</p>
Privacy	<p>The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual’s expectations; also, the right of an individual to control the collection, use, and disclosure of personal information. (Defined in the <i>NIST SP 800-32 Introduction to Public Key Technology and the Federal PKI Infrastructure</i>)</p>
Privacy Act of 1974	<p>The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.</p> <p>The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements. (Defined by <i>Department of Justice (DOJ)</i>, https://www.justice.gov/opcl/privacy-act-1974)</p>

InfoSec Term	Definition
Privacy Act Record	Any item, collection, or grouping of information about individuals that is maintained by an agency including (but not limited to) their education, financial transactions, and/or medical, criminal, or employment history and that contains their name; or it contains the identifying number, symbol, or other identifying information assigned to the individual, such as a finger or voice print or a photograph. (Defined in <i>The Privacy Act of 1974</i>)
Privacy Capability	A combination of mutually-reinforcing privacy controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals). (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Privacy Control	The administrative, technical and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Privacy Control Assessment	The testing or evaluation of privacy 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 privacy requirements for an information system or organization. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Privacy Control Assessor	The individual, group, or organization responsible for conducting a privacy control assessment. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Privacy Control Enhancements	Statements of privacy capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Privacy Control Inheritance	A situation in which an information system or application receives protection from privacy controls (or portions of privacy controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See Common Control. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)

InfoSec Term	Definition
Privacy Impact Assessment (PIA)	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Privacy Plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Privacy Requirements	Requirements levied on an organization, information program, or information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure that privacy protections are implemented in the collection, use, sharing, storage, transmittal, and disposal of information. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Privacy Threshold Analysis (PTA)	Methodology that provides information technology (IT) security professionals with a process for assessing whether a PIA is necessary. (Defined in <i>OPM Privacy Impact Assessment Guide</i>)
Privileged account	A system account with authorizations of a privileged user. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Privileged Command	A human-initiated command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Privileged User	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Procedure	An established method of accomplishing a consistent performance or result, a procedure typically can be described as the sequence of steps that will be used to execute a process. (Defined in PMBOK Guide, <i>A Guide to the Project Management Body of Knowledge, Sixth Edition</i>)
Process	A systematic series of activities directed toward causing an end result such that one or more inputs will be acted upon to create one or more outputs. (Defined in PMBOK Guide, <i>A Guide to the Project Management Body of Knowledge, Sixth Edition</i>)
Profiling	Measuring the characteristics of expected activity so that changes to it can be more easily identified. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)

InfoSec Term	Definition
Protected Health Information (PHI)	<p>Individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Individually identifiable health information is information, including demographic data, that relates to:</p> <ul style="list-style-type: none"> • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual; <p>and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security number).</p> <p>The HIPAA Privacy Rule excludes from protected health information any employment records that a covered entity maintains in its capacity as an employer, and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. (As defined in the <i>HIPAA Privacy Rule</i>)</p>
Provenance	<p>The records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables all changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)</p>
Public Information	<p>Any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)</p>
Public Key Infrastructure (PKI)	<p>The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Purge	<p>A method of sanitization that applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Qualitative Assessment	<p>A set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels. (Defined in the <i>Department of Homeland Security Risk Lexicon</i>)</p>
Quantitative Assessment	<p>Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment. (Defined in the <i>Department of Homeland Security Risk Lexicon</i>)</p>

InfoSec Term	Definition
Reciprocity	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Remote Access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external network. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Repeatability	The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments. (Defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Reproducibility	The ability of different experts to produce the same results from the same data. (Defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Residual Risk	Portion of risk remaining after security measures have been applied. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Restricted Data	All data concerning (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 [of the Atomic Energy Act of 1954]. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
Risk	<p>A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.</p> <p>Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Risk Assessment (RA)	<p>The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.</p> <p>Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Risk Assessment Methodology	<p>A risk assessment process, together with a risk model, assessment approach, and analysis approach. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)</p>
Risk Assessment Report (RAR)	<p>The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Risk Assessor	<p>The individual, group, or organization responsible for conducting a risk assessment. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Risk Executive (Function)	<p>An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)</p>
Risk Factor	<p>A characteristic used in a risk model as an input to determining the level of risk in a risk assessment. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)</p>

InfoSec Term	Definition
Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Risk Management Framework (RMF)	The six-step process established in NIST SP 800-37, which is the transformation of the previous certification and accreditation (C&A) process. The RMF changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. (Defined in NIST SP 800-37, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i>)
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Risk Model	A key component of a risk assessment methodology (in addition to assessment approach and analysis approach) that defines key terms and assessable risk factors. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Risk Response Measure	A specific action taken to respond to an identified risk. (Defined in NIST SP 800-39, <i>Managing Information Security Risk: Organization, Mission and Information System View</i>)
Role Based Access Control (RBAC)	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Root Cause Analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. (Defined in NIST SP 800-39 <i>Managing Information Security Risk: Organization, Mission and Information System View</i>)

InfoSec Term	Definition
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Scoping Considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security and privacy controls in the control baselines. Considerations include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Assessment Plan (SAP)	The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. (Defined in <i>NIST SP 800-53, Rev 4: Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Assessment Review (SAR)	Prepared by the security control assessor, this report provides the results of the assessment of the implementation of security controls identified in the System Security Plan (SSP) to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The security assessment report can also contain a list of recommended corrective actions or deficiencies identified in the security controls. Security control assessor is a new term (role) in NIST SP 800-37. Security control assessors may be called certification agents in some organizations. (Defined in <i>NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i>)
Security Attribute	An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures including, for example, records, buffers, and files within the system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Capability	A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals). (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Category (SC)	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Security Content Automated Protocol (SCAP)	A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). (Defined in <i>The Information Security Automation Program and The Security Content Automation Protocol released by the National Vulnerability Database/NIST</i>)
Security Control	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. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Security Control Assessment	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. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>) (*1 st Part of Assessment and Authorization A&A Process)
Security Control Assessor (SCA)	The individual, group, or organization responsible for conducting a security control assessment. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Control Enhancement	Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Control Families	The security control families in NIST SP 800-53, Rev 4 are closely aligned with the security-related areas in FIPS 200 specifying the minimum security requirements for protecting Federal information and information systems. Each security control family contains security controls related to the security functionality of the family. (Defined in NIST SP 800-53, Rev 4 <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)

InfoSec Term	Definition
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See Common Control. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Domain	A domain that implements a security policy and is administered by a single authority. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
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. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Impact Analysis (SIA)	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Label	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Objective	Confidentiality, integrity, or availability. (Defined in FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>)
Security Policy	A set of criteria for the provision of security services. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Policy Filter	A hardware and/or software component that performs one or more of the following functions: content verification to ensure the data type of the submitted content; content inspection, analyzing the submitted content to verify it complies with a defined policy; malicious content checker that evaluates the content for malicious code; suspicious activity checker that evaluates or executes the content in a safe manner, such as in a sandbox or detonation chamber and monitors for suspicious activity; or content sanitization, cleansing, and transformation, which modifies the submitted content to comply with a defined policy. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Security Posture	The security status of an enterprise's networks, information, and systems based on information assurance (IA) resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)

InfoSec Term	Definition
Security Requirements	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Security Technical Implementation Guidelines (STIG)	Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Semi-Quantitative Assessment	Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. (Defined in the <i>Department of Homeland Security Risk Lexicon</i>)
Senior (Agency) Information Security Officer (SAISO)	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Senior Agency Official for Privacy (SAOP)	The senior organizational official with overall organization-wide responsibility for information privacy issues. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Sensitive Compartmented Information (SCI)	Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Sensitivity	Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Service Level Agreement (SLA)	A document stating the technical performance promises made by the cloud provider, how disputes are to be discovered and handled, and any remedies for performance failures. (Defined in <i>NIST SP 800-146: Cloud Computing Synopsis and Recommendations</i>)
Signature	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)

InfoSec Term	Definition
Software	Computer Programs and associated data that may be dynamically written or modified during execution. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure ² . The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (Defined in <i>NIST SP 800-145: The NIST Definition of Cloud Computing</i>)
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Special Access Program (SAP)	A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, architectural designs) associated with an information system. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Split Tunneling	A method that routes organization-specific traffic through the SSL VPN tunnel, but routes other traffic through the remote user's default gateway. (Defined in <i>NIST SP 800-113 Guide to SSL VPN's</i>)
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Standard	A document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. (Defined in <i>NISTIR 8074, Volume 2: Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity</i>)
Standard Operating Procedure (SOP)	A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event. (Defined in <i>NIST SP 800-127: Guide to Securing WiMAX Wireless Communications</i>)

InfoSec Term	Definition
Statement of Work (SOW)	The SOW details what the developer must do in the performance of the contract. Documentation developed under the contract, for example, is specified in the SOW. Security assurance requirements, which detail many aspects of the processes the developer follows and what evidence must be provided to assure the organization that the processes have been conducted correctly and completely, may also be specified in the SOW. (Defined in <i>NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i>)
Sub-functions	Sub-functions are the basic operations employed to provide the system services within each area of operations or line of business. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Supplementation	The process of adding security controls or control enhancements to a security control baseline as part of the tailoring process (during security control selection) in order to adequately meet the organization’s risk management needs. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
Supply Chain Risk	Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Defined in OMB Circular No. A-130, <i>Managing Information as a Strategic Resource</i>)
System Development Lifecycle (SDLC)	The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (Defined in NIST SP 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>)
System of Records (SOR)	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (Defined in the Privacy Act of 1974)

InfoSec Term	Definition
System of Records Notice (SORN)	The Privacy Act requires each agency to publish a notice of its systems of records in the Federal Register. This is called a System of Record Notice (SORN) (Defined in <i>NIST SP 800-79-2: Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)</i>)
System Security Engineering	Process that captures and refines security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
System-Specific Control	A security control or privacy control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Tailoring	The process by which a security control baseline is modified based on (i) the application of scoping guidance, (ii) the specification of compensating security controls, if needed, and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (Defined in NIST SP 800-37 Rev.1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach</i>)
Telecommunications	The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control or privacy control effectiveness over time. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)

InfoSec Term	Definition
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Threat Assessment	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Threat Shifting	Response from adversaries to perceived safeguards and/or countermeasures (i.e., security controls), in which the adversaries change some characteristic of their intent to do harm in order to avoid and/or overcome those safeguards/countermeasures. (As defined in NIST SP 800-30 Rev.1, <i>Guide for Conducting Risk Assessments</i>)
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. (Defined in NIST SP 800-53 Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)
Trustworthiness	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Unique Item Identifier (UII)	A globally unique and unambiguous set of data elements marked on items. The UII is derived from a UII data set of one or more data elements. The term includes a concatenated unique item identifier or a Department of Defense (DoD) recognized unique identification equivalent. (Defined at <i>Defense Acquisition Glossary</i> , https://www.dau.mil/glossary/pages/2837.aspx)
United States Computer Emergency Readiness Team (US-CERT)	A partnership between the Department of Homeland Security (DHS) and the public and private sectors, established to protect the nation's internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
United States Government Configuration Baseline (USGCB)	The United States Government Configuration Baseline (USGCB) provides security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the federal Desktop Core Configuration mandate. (Defined at <i>NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems</i>)

InfoSec Term	Definition
User	Individual, or (system) process acting on behalf of an individual, who is authorized to access an information system. (Defined in CNSSI 4009, <i>Committee on National Security Systems Glossary</i>)
Virtual Private Network (VPN)	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Voice Over Internet Protocol (VOIP)	Equipment that provides the ability to dial telephone numbers and communicate with parties on the other end of a connection who have either another VOIP system or a traditional analog telephone. (Defined in NIST SP 800-58, <i>Security Considerations for Voice Over IP Systems</i>)
Vulnerability	<p>Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Defined in NIST SP 800-53A Rev.4, <i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>)</p> <p>A weakness in a system, application, or network that is subject to exploitation or misuse. (Defined in NIST 800-61 Rev 2, <i>Computer Security Incident Handling Guide</i>)</p>
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
Weapons System	A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (Defined in NIST SP 800-60 Vol.1 Rev.1, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>)
Web Measurement and Customization Technology	Technologies used to remember a user’s online interactions with a Website or online application in order to conduct measurement and analysis of usage or to customize the user’s experience. This term may be associated with the term cookie. (Defined in OMB M-10-22, <i>Guidance for Online Use of Web Measurement and Customization Technologies</i>)
Whitelisting	The process used to identify software programs that are authorized to execute on an information system; or authorized Universal Resource Locators or websites. (Defined in NIST SP 800-53 Rev.4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>)
WiFi or Wi-Fi	Trademarked term meaning IEEE 802.11x and is the common name of a wireless networking technology that uses radio waves to provide high-speed network and Internet connections. The term may also be used interchangeably for “wireless” and/or “wireless fidelity,” however, these are not the original meaning of the term. (Defined in Webopedia, <i>Wi-Fi (wireless networking)</i> , 2018)

InfoSec Term	Definition
Wireless Local Area Network (WLAN)	A group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). (Defined in NIST SP 800-46, <i>Security for Telecommuting and Broadband Communications</i>)

8 Appendix F: Minimum Set of HHS and NIH Roles Assigned Significant Responsibilities for Information Security

Both the Federal Information Security Management Act (FISMA) and the Office of Personnel Management (OPM) Regulation 5 Code of Federal Regulations (CFR) 930.301 require federal agencies to:

- Identify personnel with significant security responsibilities; and
- Provide security training commensurate with these responsibilities in the form of role-based training.

Additionally, the requirements within this Handbook are consistent with the HHS IS2P. Within the HHS and NIH environments, significant security responsibilities are defined as the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security posture of one or more HHS or NIH systems. As such, the following roles, consistent with OPM Regulation 5 CFR 930.301 represent the *minimum* set of roles at HHS and NIH that possess significant security responsibilities. Each role is characterized by its population - both mandatory and optional members - and relevant responsibilities. These individuals include:

1. Executives

Mandatory Population:

- All members of the Senior Executive Service (SES).

Optional Population:

- None specified.

Relevant Responsibilities:

- Formulation of policy and guidance that may impact information system and/or security policy and operations.
- Allocation of resources to manage enterprise risk related to the use of information and information systems.

2. Chief Information Officers and Chief Information Security Officers

Mandatory Population:

- HHS CIO, direct managerial reports and component organizations, NIH and IC CIOs, direct managerial reports and component organizations, HHS CISO, and NIH and IC CISOs.

Optional Population:

- None specified.

Relevant Responsibilities:

- Establishment of information security and/or system policy.
- Management of the IT function and related risks.

3. IT Security Program Managers

Mandatory Population:

- Individuals with the titles of Information Systems Security Officer (ISSO), Information Security Officer (ISO), or System Security Officer (SSO) and their information security employees or contractors.
- All information security employees or contractors working for or contracted by the HHS CISO or the NIH CISO.

Optional Population:

- Positions within the GS-2210 Information Technology Management job series might fill this role.

Relevant Responsibilities:

- Implementation of information security policies.

4. Program and Functional Managers/Information Technology (IT) Functional Management and Operations Personnel

Mandatory Population:

- All personnel identified as a System Owner, Data Steward, Data Owner, Program Manager, or Project Manager.

Optional Population:

- Positions within the following series that might fill this role: GS-0332 Computer Operator, GS-0334 Computer Specialist, GS-2210 Information Technology Management, GS-0340 Program Management Series, and GS-0343, Management and Program Analysis.

Relevant Responsibilities:

- Stewardship of a system or its information assets during its development and/or operation.

5. IT Auditors

Mandatory Population:

- All personnel engaged in the auditing of HHS or NIH information technology systems or networks.

Optional Population:

- Positions within the GS-0511 Auditing job series might fill this role.

Relevant Responsibilities:

- Evaluation of systems for appropriate and effective implementation of controls to address security risks.

6. Other Security-Oriented Personnel

Mandatory Population:

- Information Technology (IT) administrators (e.g., network administrators, system administrators, and database administrators).

Optional Population:

- Positions within the GS-1550 Computer Science or the GS-0391 Telecommunications job series might fill this role.

Relevant Responsibilities:

- Enable the implementation and operation of one or more system security controls, as outlined in *NIST SP 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations* (as amended).

NIH and ICs must identify employees and contractors who hold the aforementioned roles or responsibilities. The performance of this identification process is considered the completion of an NIH Personnel Needs Assessment. Personnel whose responsibilities are not captured within this appendix but meet the intent of the significant security responsibilities definition must also be designated. Personnel whose job duties meet these criteria must complete the HHS' RBT course(s) associated with their role. Personnel that assume multiple roles must complete training that addresses the unique risks associated with each role. However, this training may be combined at the NIH's discretion. HHS RBT courses can be located at http://intranet.hhs.gov/it/cybersecurity/training/role_based/index.html.

Alternatively, NIH may provide equivalent RBT to address the aforementioned roles, or combination of roles, with significant security responsibilities. Individuals beginning work with NIH or IC must be required to complete the appropriate RBT within three months of their initial start date.

9 Appendix G: System Component Inventory Requirements

As defined in the Configuration Management (CM) control family, specifically CM-8, organizations must develop and document a component inventory for all information systems. The inventory must include all components within the authorization boundary of the information system and be at the level of granularity deemed necessary for tracking and reporting. At a minimum, the inventory record for each system component must include the following information:

- Unique identifier and/or serial number;
- System name of which the component is a part;
- Type of system component (e.g., server, desktop, network device, storage, application);
- Manufacturer/model;
- Operating system type and version/service pack level;
- Presence of virtual machines;
- Application software version/license information;
- Physical location (e.g., building/room number);
- Logical location (e.g., IP address);
- Media Access Control (MAC) address;
- Owner;
- Operational status; and
- Primary and secondary administrators.

10 Appendix H: Information System Media

As required by the Media Protection (MP) control family, organizations must physically control and restrict access to information system media. The term “information system media” includes, but is not limited to, the types and examples listed in the table below. Applicable restrictions are listed in the far-right columns, depending on the FIPS 199 security classification of the system that uses the media.

Media Type	Examples	Restrictions		
		Low	Moderate	High
Hard Copy Storage	<ul style="list-style-type: none"> Paper Microforms 	--	Depends on sensitivity and whether PII is present.	
Mobile Devices	<ul style="list-style-type: none"> Laptops Cell phones and smart phones (e.g., iPhone, Android, BlackBerry) E-readers (e.g., Kindle) Tablets (e.g., iPad) 	Government-furnished devices must be encrypted, with waivers being required for any exceptions. Personally-owned devices must adhere to NIH policies. All devices must implement NIH identification and authentication controls.		
Equipment	<ul style="list-style-type: none"> Photocopiers Printers Fax machines Multifunction machines 	--	If it contains a storage device, media disposal and sanitization rules apply. Consult SP 800-88 for more information.	
Legacy Magnetic Media	<ul style="list-style-type: none"> Magnetic tapes (e.g., backup tapes) ATA and SCSI hard drives Floppy disks ZIP drives 	--	Not allowed unless they can be stored in NIH controlled environments.	
Peripherally Attached Storage	<ul style="list-style-type: none"> Removable hard drives Locally attached hard drives (attached via USB, Firewire, etc.) 	Personally-owned devices in this category are prohibited.		
Optical Media	<ul style="list-style-type: none"> Compact Discs (CDs) Digital Video Discs (DVDs) Blu-ray 	--	All discs must be encrypted.	
Flash-Based Storage Devices	<ul style="list-style-type: none"> USB removable media (e.g., thumb drives, memory sticks) Memory cards (e.g., SD, SDHC, MMC, Compact Flash) ATA Solid State Drives (SSDs) SCSI Solid State Drives (SSDs) PCI Express Devices Embedded Flash on Boards and Devices 	Personally-owned devices in this category are prohibited.		
RAM and ROM-Based Storage Devices	<ul style="list-style-type: none"> Dynamic Random Access Memory (DRAM) Electrically Alterable PROM (EAPROM) Electrically Erasable PROM (EEPROM) 	Personally-owned devices in this category are prohibited.		

END OF DOCUMENT