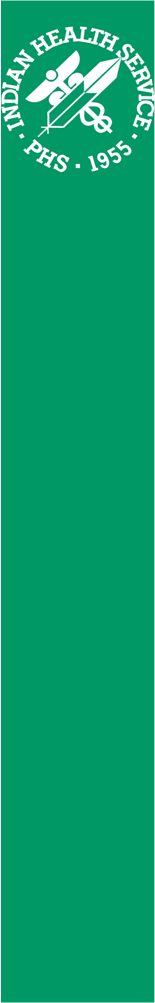
|  |  |
| --- | --- |
|  | HHS Logo |

Indian Health Service (IHS)

*Instruction: This template includes instructions and example text for various sections. Users of this document should consider using the find and replace function to populate common information such as <<System Acronym>>.*

Security Assessment Plan (SAP)

For <<Name of System>> <<(System Acronym)>>

Security Categorization: <<Low, Moderate, High>>

<<Authorization to Operate (ATO), Annual Assessment (Year 1 or 2), Significant Change>>

*Instruction: The SAP date should be modified to reflect the most recent update and approval of this document.*

<<*Month*>> <<*Year*>>

CONTROLLED UNCLASSIFIED INFORMATION (CUI) - This information is intended for IHS use only. Disclosure may cause harm to the IHS. Access is provided by request only.

Approval

I have reviewed and approve this <<System Acronym>> Security Assessment Plan.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| << Insert Name >>  System Owner | Date |

Table of Contents

[Approval i](#_Toc450147752)

[Table of Contents ii](#_Toc450147753)

[Record of Changes iii](#_Toc450147754)

[1. Introduction 1](#_Toc450147755)

[1.1 Background 1](#_Toc450147756)

[1.2 Purpose 1](#_Toc450147757)

[2. System Overview 2](#_Toc450147758)

[2.1 System Identification 2](#_Toc450147759)

[2.1.1 System Type 2](#_Toc450147760)

[2.1.2 Operational Status 3](#_Toc450147761)

[2.2 Designated Contacts 4](#_Toc450147762)

[3. Security Assessment & Authorization Plan 5](#_Toc450147763)

[3.1 Risk Management Framework (RMF) 5](#_Toc450147764)

[3.2 Assessment Purpose 5](#_Toc450147765)

[3.3 Assessment Type 5](#_Toc450147766)

[3.4 Assessment / ATO Cycle 5](#_Toc450147767)

[3.5 Assessment Milestones 6](#_Toc450147768)

[3.6 Assessment Methods 7](#_Toc450147769)

[3.7 Control Tailoring 7](#_Toc450147770)

[3.8 Assessment Scope 7](#_Toc450147771)

[3.9 Manual Checklists 8](#_Toc450147772)

[3.10 Automated Tools 8](#_Toc450147773)

[3.11 Baseline Configuration Standards 8](#_Toc450147774)

[3.12 Risk Determination 8](#_Toc450147775)

[Appendix A. Security Controls 10](#_Toc450147776)

[Appendix B. Applicable Laws and Regulations 18](#_Toc450147777)

[Appendix C. Acronyms 20](#_Toc450147778)

Record of Changes

*Note: Throughout this template, red italicized text is provided to show an example of the data that users should include.*

| Date | Description | Author |
| --- | --- | --- |
| *1/1/2015* | *Created initial draft, including basic system information from the SSP.* | *J. Smith* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Introduction

## Background

The Federal Information Security Modernization Act (FISMA) of 2014, requires each federal agency to develop, document, and implement an agency-wide information security program to safeguard the data and information technology (IT) systems that support the operations and assets of the agency. System security planning is an important activity in the agency’s security program and should be incorporated throughout a system’s lifecycle. This planning helps ensure that events such as system changes or new threats that trigger updates to security controls can be accurately documented and effectively managed. A critical component of meeting this requirement is planning for, and conducting periodic assessments of, risk to agency operations or assets resulting from the operation of information systems.

## Purpose

The primary purpose of this document is to establish the appropriate expectations for the security control assessment of <<System Acronym>> by providing a detailed roadmap of how the assessment will be conducted, the level of effort required to complete the assessment, and the overall scope and purpose of the assessment.

In addition to its primary purpose, using this plan will contribute to IHS’s ability to comply with a number of laws, memoranda, standards, and guidelines including FISMA, Office of Management and Budget (OMB) *Circular A-130, Appendix III*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2*, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

# System Overview

This section provides information about <<System Acronym>> that is critical to conducting an accurate and thorough security control assessment. The <<System Acronym>> System Security Plan (SSP) is the primary source for system information and detailed descriptions of the security controls that have been implemented to protect the system and its data. The Security Control Assessor will evaluate all information provided by the <<System Acronym>> SSP during this assessment.

## System Identification

This section contains information identifying the <<System Acronym>> system. Table 1 contains the <<System Acronym>> system name, per the Health and Human Services (HHS) Enterprise Architecture Repository (HEAR).

*Instruction: Complete the table below with applicable information from the HEAR.*

Table 1: Information System Name and Title

|  |  |  |
| --- | --- | --- |
| **Universal Unique Identifier (UUID)** | **Information System Name** | **Information System Acronym** |
| *IHS-0123456* | *Example IHS System* | *EIS* |

### System Type

Table 2 indicates the <<System Acronym>> system type.

*Instruction: Select the applicable information system type from the table below. To select, double click the applicable gray box below. In the “Default value” section of the Check Box Form Field dialogue box, select “Checked.” Then click on the “OK” button.*

Table 2: Information System Type

|  |  |
| --- | --- |
| **System Type Selection** | |
|  | **General Support System (GSS)** |
|  | **Major Application** |
|  | **Minor Application** |

### Operational Status

The system is currently in the life-cycle phase noted in Table 3.

*Instruction: Select all status indicators that apply. If selecting more than one status, list which components of the system apply to each status in the space below the table. To select, double click the applicable gray box below. In the “Default value” section of the Check Box Form Field dialogue box, select “Checked.” Then click on the “OK” button.*

Table 3: Current System Status

| **Current System Status** | | |
| --- | --- | --- |
|  | **Under Development** | The system is being designed, developed, or implemented. |
|  | **Operational** | The system is in production. |
|  | **Undergoing Major Modification** | The system is undergoing a major conversion or transition. |

## Designated Contacts

The individual(s) identified below are responsible for the management, operation, security, and authorization of the system.

*Instruction: Add additional rows as needed.*

Table 4: Designated Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Title or Role** | **Name** | **Phone** | **E-mail** |
| **Information System Owner** |  |  |  |
| **Business / Data Owner** |  |  |  |
| **Project / Program Manager** |  |  |  |
| **Investment / CPIC Manager** |  |  |  |
| **Technical POC** |  |  |  |
| **Information System Security Officer (ISSO)** |  |  |  |
| **Security Control Assessor** |  |  |  |
| **Chief Information Security Officer (CISO)** | CDR Steven Miller | 301-443-2452 | Steven.miller@ihs.gov |
| **Authorizing Official (AO)** | Mitchell Thornbrugh | 301-443-2019 | Mitchell.thornbrugh@ihs.gov |

# Security Assessment & Authorization Plan

Security control assessment and system authorization is required by FISMA, and is practiced by all agencies across the Federal Government. In accordance with FISMA, NIST has developed standards and guidelines for the documentation, assessment, and authorization of federal information systems. The IHS Security Assessment & Authorization (SA&A) process allows IHS Security Control Assessors and system stakeholders to identify and document risks to individual IHS systems and the IHS enterprise as a whole.

The following sections describe key characteristics of the IHS SA&A process and are applicable to all security control assessments of IHS information systems.

## Risk Management Framework (RMF)

The IHS SA&A process has been modeled after the tasks defined in NIST SP 800-37, Revision 2. A comprehensive description of each task in the IHS SA&A process is available upon request by email to the IHS Risk & Compliance (R&C)Team.

## Assessment Purpose

The purpose of the security control assessment is to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

## Assessment Type

*Instruction: Describe the type of assessment to be conducted. Indicate if this is a new ATO, Annual (including which year), Re-ATO, or significant change assessment. If this is a significant change assessment, describe the changes that will be included in the scope of this assessment. Also note whether this is a type accreditation.*

## Assessment / ATO Cycle

System owners must complete a detailed security control assessment and subsequent Authorization to Operate (ATO) before placing an information system into production. It is the intent of the IHS R&C Team to conduct initial security control assessments in parallel with the development/acquisition and implementation phases of the system development life cycle. This allows the Security Control Assessor to identify weaknesses as early as possible and provide the most cost-effective method for initiating corrective actions.

A standard ATO is valid for a three year period, or until a significant change to the system occurs. The standard authorization period may be adjusted if needed and must be clearly stated on the Authorization Decision Document, or ATO Memo. After the Authorizing Official (AO) grants the initial ATO, the Security Control Assessor assesses one third of all applicable security controls each subsequent year. Every third year, System stakeholders use these assessments as basis for a new ATO. Figure 1 depicts the standard three-year ATO cycle.

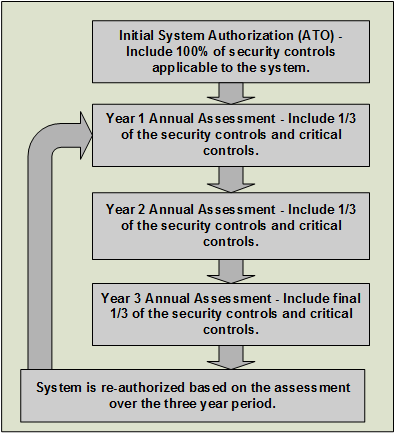


Figure 1: Standard Three Year ATO Cycle

## Assessment Milestones

Table 5: Assessment Milestones lists the key tasks for conducting the security assessment of <<System Acronym>> and a target completion date for each task.

*Instruction: Ensure that all parties agree to the dates in the table below.*

Table 5: Assessment Milestones

|  |  |
| --- | --- |
| **Milestone** | **Target Completion Date** |
| Assessment Kick-Off Meeting |  |
| Initial Security Documents Received |  |
| Security Assessment Plan Developed |  |
| Initial Assessment Meeting |  |
| Final Assessment Meeting |  |
| Final Vulnerability & Configuration Scans |  |
| Findings Meeting |  |
| Security Assessment Report (SAR) Submitted for Review & Approval |  |

## Assessment Methods

Security Control Assessors will use the following processes to assess <<System Acronym>>:

* Examination: Analyzing documentation (e.g., policies, plans, procedures, system requirements, designs) to facilitate understanding, get clarification, or obtain evidence to support the determination of security and privacy control existence and effectiveness.
* Interview: Conducting discussions with individuals or groups within an organization or system to facilitate understanding, get clarification, or lead to the location of evidence to support the determination of security and privacy control existence and effectiveness.
* Test: Assessing system mechanisms or activities under specified conditions to support the determination of security and privacy control existence and effectiveness.

## Control Tailoring

As stated in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* organizations use tailoring to appropriately modify and align the security controls selected for an information system with specific conditions and security requirements of the system and IHS. Tailoring a security control baseline may mean adding, removing, or modifying controls. System stakeholders may tailor controls in the following ways:

* Add controls if additional security requirements, above those in the initial security control baseline, are needed.
* Remove controls that are not applicable to the system, for example SC-19, Voice over Internet Protocol (VOIP).
* Modify controls if the security control parameter must be adjusted due to operational or technical requirements.

System owners must document all control tailoring in the <<System Acronym>> SSP. The Security Control Assessor will validate all control tailoring during this assessment.

## Assessment Scope

The scope of this security assessment includes only those components identified in the “Authorization Boundary” section of the system’s SSP.

*Instruction: This statement should be adjusted according to the type of assessment being conducted. A significant change assessment may target only specific components of the system.*

Appendix A of this document lists each of the security controls that will be tested during this assessment.

*Instruction: If this is a type accreditation assessment clarify what components, processes, etc. will be included in this assessment and which will not.*

## Manual Checklists

This security assessment will use the IHS’s Security Test and Evaluation (ST&E) worksheet. The IHS developed this checklist based on guidance from NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* and the checklist includes all controls that will be tested during this assessment. Appendix A of this report includes a complete list of security controls.

## Automated Tools

During this assessment, the Security Control Assessor will use the following automated tools to identify security vulnerabilities in the <<System Acronym>> information system:

* Nessus vulnerability scanner
* Local PowerShell/WMI scripts
* <<List any other automated tools to be used>>

*Instruction: This list should be modified as appropriate for the assessment. List only those tools that are going to be used.*

## Baseline Configuration Standards

The Security Control Assessor will use all available IHS configuration standards and/or hardening guides that are applicable to <<System Acronym>> during this assessment.

## Risk Determination

The Security Control Assessor will document all security risks identified during the assessment and indicate the level of risk based on the guidance below.

As stated in NIST SP 800-37, Revision 2, “Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event Risk is also a function of the adverse impacts that arise if the circumstance or event occurs, and the likelihood of occurrence.” IHS Security Control Assessors will use the following tables to assist in the analysis and documentation of risk.

Table 6: Impact Definitions

| **Impact** | **Description** |
| --- | --- |
| Low | If vulnerabilities are exploited by threats, little to no loss to the system, networks, or data would occur. |
| Moderate | If vulnerabilities are exploited by threats, moderate loss to the system, networks, and data would occur. |
| High | If vulnerabilities are exploited by threats, significant loss to the system, networks, and data would occur. |

Table 7: Likelihood Definitions

| **Likelihood** | **Description** |
| --- | --- |
| Low | There is little to no chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| Moderate | There is a moderate chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| High | There is a high chance that a threat could exploit a vulnerability and cause loss to the system or its data. |

Table 8: Risk Ratings

| **Likelihood** | **Impact** | | |
| --- | --- | --- | --- |
| **Low** | **Medium** | **High** |
| High | Low | Medium | High |
| Medium | Low | Medium | Medium |
| Low | Low | Low | Low |

Appendix A. Security Controls

*Instruction: Select the appropriate text below. For a full assessment in which all NIST 800-53 controls will be tested, simply delete the 2nd sentence below and select the appropriate categorization from the 1st sentence. For an annual or targeted assessment, delete the 1st sentence below and delete from the chart any rows for controls that won’t be tested during this assessment.*

For this security assessment, all controls in the chart below that are applicable to the <<low, moderate, high>> baseline will be tested.

For this security assessment, all controls listed in the chart below will be tested.

The following schedule has been developed in order to ensure that all controls applicable to a system are assessed in the three year authorization period.

Critical controls have been identified based on their importance to the security of IHS information and information systems. These controls were selected based on the SANS *Critical Security Controls for Effective Cyber Defense*. Critical controls are tested annually at minimum.

Table 7 – Security Control Assessment Schedule

| ID | Control Description | Sensitivity Level | | | Assessment Year |
| --- | --- | --- | --- | --- | --- |
| Low | Mod | High |
| Access Control | | | | |  |
| AC-1 | Access Control Policy & Procedures | AC-1 | AC-1 | AC-1 | 3 |
| AC-2 | Account Management | AC-2 | AC-2, (1) (2) (3) (4) | AC-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-2#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-2#enhancement-3) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-2#enhancement-4) (5) (12) (13) | 1, 2, 3 |
| AC-3 | Access Enforcement | AC-3 | AC-3 | AC-3 | 1, 2, 3 |
| AC-4 | Information Flow Enforcement | Not Selected | AC-4 | AC-4 | 1 |
| AC-5 | Separation of Duties | Not Selected | AC-5 | AC-5 | 1 |
| AC-6 | Least Privilege | Not Selected | AC-6 (1) (2) (5) (9) (10) | AC-6 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-6#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-6#enhancement-2) (3) (5) (9) (10) | 1, 2, 3 |
| AC-7 | Unsuccessful Login Attempts | AC-7 | AC-7 | AC-7 | 1 |
| AC-8 | System Use Notification | AC-8 | AC-8 | AC-8 | 1 |
| AC-10 | Concurrent Session Control | Not Selected | Not Selected | AC-10 | 1 |
| AC-11 | Session Lock | Not Selected | AC-11 (1) | AC-11 (1) | 1 |
| AC-12 | Session Termination | Not Selected | AC-12 | AC-12 | 1 |
| AC-14 | Permitted Actions without Identification or Authentication | AC-14 | AC-14 | AC-14 | 1 |
| AC-17 | Remote Access | AC-17 | AC-17 (1) (2) (3) (4) | AC-17 (1) (2) (3) (4) | 1, 2, 3 |
| AC-18 | Wireless Access | AC-18 | AC-18 (1) | AC-18 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-18#enhancement-1) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-18#enhancement-4) [(5)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-18#enhancement-5) | 1, 2, 3 |
| AC-19 | Access Control for Mobile Devices | AC-19 | AC-19 (5) | AC-19 [(5)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-19#enhancement-1) | 1 |
| AC-20 | Use of External Information Systems | AC-20 | AC-20 (1) (2) | AC-20 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-20#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=AC-20#enhancement-2) | 1 |
| AC-21 | Information Sharing | Not Selected | AC-21 | AC-21 | 1 |
| AC-22 | Publicly Accessible Content | AC-22 | AC-22 | AC-22 | 1 |
| Awareness and Training | | | | |  |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | AT-1 | AT-1 | 1 |
| AT-2 | Security Awareness Training | AT-2 | AT-2 (2) | AT-2 (2) | 1, 2, 3 |
| AT-3 | Role-Based Security Training | AT-3 | AT-3 | AT-3 | 1, 2, 3 |
| AT-4 | Security Training Records | AT-4 | AT-4 | AT-4 | 1 |
| Audit and Accountability | | | | |  |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | AU-1 | AU-1 | 1 |
| AU-2 | Audit Events | AU-2 | AU-2 (3) | AU-2 [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-2#enhancement-3) | 1, 2, 3 |
| AU-3 | Content of Audit Records | AU-3 | AU-3 (1) | AU-3 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-3#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-3#enhancement-2) | 1, 2, 3 |
| AU-4 | Audit Storage Capacity | AU-4 | AU-4 | AU-4 | 1 |
| AU-5 | Response to Audit Processing Failures | AU-5 | AU-5 | AU-5 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-5#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-5#enhancement-2) | 1 |
| AU-6 | Audit Review, Analysis, and Reporting | AU-6 | AU-6 (1) (3) | AU-6 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-6#enhancement-1) (3) (5) (6) | 1, 2, 3 |
| AU-7 | Audit Reduction and Report Generation | Not Selected | AU-7 (1) | AU-7 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-7#enhancement-1) | 1 |
| AU-8 | Time Stamps | AU-8 | AU-8 (1) | AU-8 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-8#enhancement-1) | 1 |
| AU-9 | Protection of Audit Information | AU-9 | AU-9 (4) | AU-9 (2) (3) (4) | 1 |
| AU-10 | Non-repudiation | Not Selected | Not Selected | AU-10 | 1 |
| AU-11 | Audit Record Retention | AU-11 | AU-11 | AU-11 | 1 |
| AU-12 | Audit Generation | AU-12 | AU-12 | AU-12 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=AU-12#enhancement-1) (3) | 1 |
| Security Assessment and Authorization | | | | |  |
| CA-1 | Security Assessment and Authorization Policies & Procedures | CA-1 | CA-1 | CA-1 | 3 |
| CA-2 | Security Assessments | CA-2 | CA-2 (1) | CA-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CA-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CA-2#enhancement-2) | 1 |
| CA-3 | System Interconnections | CA-3 | CA-3 (5) | CA-3 (5) | 1 |
| CA-5 | Plan of Action & Milestones | CA-5 | CA-5 | CA-5 | 1, 2, 3 |
| CA-6 | Security Authorization | CA-6 | CA-6 | CA-6 | 1 |
| CA-7 | Continuous Monitoring | CA-7 | CA-7 (1) | CA-7 (1) | 1, 2, 3 |
| CA-8 | Penetration Testing | Not Selected | Not Selected | CA-8 | 1 |
| CA-9 | Internal System Connections | CA-9 | CA-9 | CA-9 | 1 |
| Configuration Management | | | | |  |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 | CM-1 | 3 |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (1) (3) (7) | CM-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-2#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-2#enhancement-3) [(7)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-2#enhancement-5) | 2 |
| CM-3 | Configuration Change Control | Not Selected | CM-3 (2) | CM-3 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-3#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-3#enhancement-2) | 2 |
| CM-4 | Security Impact Analysis | CM-4 | CM-4 | CM-4 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-4#enhancement-1) | 2 |
| CM-5 | Access Restrictions for Change | Not Selected | CM-5 | CM-5 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-5#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-5#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-5#enhancement-3) | 1 |
| CM-6 | Configuration Settings | CM-6 | CM-6 | CM-6 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-6#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-6#enhancement-2) | 1, 2, 3 |
| CM-7 | Least Functionality | CM-7 | CM-7 (1) (2) (4) | CM-7 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-7#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-7#enhancement-2) (5) | 1, 2, 3 |
| CM-8 | Information System Component Inventory | CM-8 | CM-8 (1) (3) (5) | CM-8 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-8#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-8#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-8#enhancement-3) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-8#enhancement-4) [(5)](http://web.nvd.nist.gov/view/800-53/control?controlName=CM-8#enhancement-5) | 1, 2, 3 |
| CM-9 | Configuration Management Plan | Not Selected | CM-9 | CM-9 | 2 |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 | CM-10 | 2 |
| CM-11 | User-Installed Software | CM-11 | CM-11 | CM-11 | 2 |
| Contingency Planning | | | | |  |
| CP-1 | Contingency Planning Policy & Procedures | CP-1 | CP-1 | CP-1 | 3 |
| CP-2 | Contingency Plan | CP-2 | CP-2 (1) (3) (8) | CP-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-2#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-2#enhancement-3) (4) (5) (8) | 1, 2, 3 |
| CP-3 | Contingency Training | CP-3 | CP-3 | CP-3 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-3#enhancement-1) | 2 |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 (1) | CP-4 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-4#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-4#enhancement-2) | 2 |
| CP-6 | Alternate Storage Site | Not Selected | CP-6 (1) (3) | CP-6 (1) (2) (3) | 2 |
| CP-7 | Alternate Processing Site | Not Selected | CP-7 (1) (2) (3) | CP-7 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-7#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-7#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-7#enhancement-3) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-7#enhancement-4) | 2 |
| CP-8 | Telecommunications Services | Not Selected | CP-8 (1) (2) | CP-8 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-8#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-8#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-8#enhancement-3) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-8#enhancement-4) | 2 |
| CP-9 | Information System Backup | CP-9 | CP-9 (1) | CP-9 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-9#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-9#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-9#enhancement-3) (5) | 1, 2, 3 |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | CP-10 (2) | CP-10 [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-10#enhancement-2) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=CP-10#enhancement-4) | 2 |
| Identification and Authentication | | | | |  |
| IA-1 | Identification and Authentication Policy & Procedures | IA-1 | IA-1 | IA-1 | 3 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (12) | IA-2 (1) (2) (3) (8) (11) (12) | IA-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-2#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-2#enhancement-3) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-2#enhancement-4) [(8)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-2#enhancement-8) [(9)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-2#enhancement-9) (11) (12) | 1, 2, 3 |
| IA-3 | Device Identification and Authentication | Not Selected | IA-3 | IA-3 | 2 |
| IA-4 | Identifier Management | IA-4 | IA-4 | IA-4 | 2 |
| IA-5 | Authenticator Management | IA-5 (1) (11) | IA-5 (1) (2) (3) (11) | IA-5 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-5#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-5#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=IA-5#enhancement-3) (11) | 2 |
| IA-6 | Authenticator Feedback | IA-6 | IA-6 | IA-6 | 2 |
| IA-7 | Cryptographic Module Authentication | IA-7 | IA-7 | IA-7 | 2 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | 2 |
| Incident Response | | | | |  |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 | IR-1 | 3 |
| IR-2 | Incident Response Training | IR-2 | IR-2 | IR-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-2#enhancement-2) | 1 |
| IR-3 | Incident Response Testing | Not Selected | IR-3 (2) | IR-3 [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-3#enhancement-1) | 1 |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) | IR-4 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-4#enhancement-1) (4) | 1 |
| IR-5 | Incident Monitoring | IR-5 | IR-5 | IR-5 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-5#enhancement-1) | 1, 2, 3 |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) | IR-6 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-6#enhancement-1) | 1, 2, 3 |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1) | IR-7 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=IR-7#enhancement-1) | 1 |
| IR-8 | Incident Response Plan | IR-8 | IR-8 | IR-8 | 1 |
| Maintenance | | | | |  |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | MA-1 | MA-1 | 2 |
| MA-2 | Controlled Maintenance | MA-2 | MA-2 | MA-2 [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=MA-2#enhancement-2) | 2 |
| MA-3 | Maintenance Tools | Not Selected | MA-3 (1) (2) | MA-3 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=MA-3#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=MA-3#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=MA-3#enhancement-3) | 2 |
| MA-4 | NonLocal Maintenance | MA-4 | MA-4 (2) | MA-4 [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=MA-4#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=MA-4#enhancement-3) | 2 |
| MA-5 | Maintenance Personnel | MA-5 | MA-5 | MA-5 (1) | 2 |
| MA-6 | Timely Maintenance | Not Selected | MA-6 | MA-6 | 2 |
| Media Protection | | | | |  |
| MP-1 | Media Protection Policy and Procedures | MP-1 | MP-1 | MP-1 | 2 |
| MP-2 | Media Access | MP-2 | MP-2 | MP-2 | 2 |
| MP-3 | Media Marking | Not Selected | MP-3 | MP-3 | 2 |
| MP-4 | Media Storage | Not Selected | MP-4 | MP-4 | 2 |
| MP-5 | Media Transport | Not Selected | MP-5 (4) | MP-5 [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=MP-5#enhancement-4) | 2 |
| MP-6 | Media Sanitization | MP-6 | MP-6 | MP-6 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=MP-6#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=MP-6#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=MP-6#enhancement-3) | 2 |
| MP-7 | Media Use | MP-7 | MP-7 (1) | MP-7 (1) | 2 |
| MP-8 | Media Downgrading | Not Selected | Not Selected | Not Selected |  |
| Physical and Environmental Protection | | | | |  |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | PE-1 | PE-1 | 2 |
| PE-2 | Physical Access Authorizations | PE-2 | PE-2 | PE-2 | 1, 2, 3 |
| PE-3 | Physical Access Control | PE-3 | PE-3 | PE-3 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-3#enhancement-1) | 2 |
| PE-4 | Access Control for Transmission Mission | Not Selected | PE-4 | PE-4 | 2 |
| PE-5 | Access Control for Output Devices | Not Selected | PE-5 | PE-5 | 2 |
| PE-6 | Monitoring Physical Access | PE-6 | PE-6 (1) | PE-6 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-6#enhancement-1) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-6#enhancement-2) | 2 |
| PE-8 | Visitor Access Records | PE-8 | PE-8 | PE-8 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-8#enhancement-1) | 1, 2, 3 |
| PE-9 | Power Equipment and Cabling | Not Selected | PE-9 | PE-9 | 2 |
| PE-10 | Emergency Shutoff | Not Selected | PE-10 | PE-10 | 2 |
| PE-11 | Emergency Power | Not Selected | PE-11 | PE-11 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-11#enhancement-1) | 2 |
| PE-12 | Emergency Lighting | PE-12 | PE-12 | PE-12 | 2 |
| PE-13 | Fire Protection | PE-13 | PE-13 (3) | PE-13 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-13#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-13#enhancement-2) [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-13#enhancement-3) | 2 |
| PE-14 | Temperature and Humidity Controls | PE-14 | PE-14 | PE-14 | 2 |
| PE-15 | Water Damage Protection | PE-15 | PE-15 | PE-15 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=PE-15#enhancement-1) | 2 |
| PE-16 | Delivery and Removal | PE-16 | PE-16 | PE-16 | 2 |
| PE-17 | Alternate Work Site | Not Selected | PE-17 | PE-17 | 2 |
| PE-18 | Location of Information System Components | Not Selected | Not Selected | PE-18 | 2 |
| Planning | | | | |  |
| PL-1 | Security Planning Policy and Procedures | PL-1 | PL-1 | PL-1 | 3 |
| PL-2 | System Security Plan | PL-2 | PL-2 (3) | PL-2 (3) | 1, 2, 3 |
| PL-4 | Rules of Behavior | PL-4 | PL-4 (1) | PL-4 (1) | 3 |
| PL-8 | Information Security Architecture | Not Selected | PL-8 | PL-8 | 3 |
| Personnel Security | | | | |  |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | PS-1 | PS-1 | 3 |
| PS-2 | Position Risk Designation | PS-2 | PS-2 | PS-2 | 3 |
| PS-3 | Personnel Screening | PS-3 | PS-3 | PS-3 | 3 |
| PS-4 | Personnel Termination | PS-4 | PS-4 | PS-4 (2) | 3 |
| PS-5 | Personnel Transfer | PS-5 | PS-5 | PS-5 | 3 |
| PS-6 | Access Agreements | PS-6 | PS-6 | PS-6 | 3 |
| PS-7 | Third-Party Personnel Security | PS-7 | PS-7 | PS-7 | 3 |
| PS-8 | Personnel Sanctions | PS-8 | PS-8 | PS-8 | 3 |
| Risk Assessment | | | | |  |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | RA-1 | RA-1 | 3 |
| RA-2 | Security Categorization | RA-2 | RA-2 | RA-2 | 1, 2, 3 |
| RA-3 | Risk Assessment | RA-3 | RA-3 | RA-3 | 1,2,3 |
| RA-5 | Vulnerability Scanning | RA-5 | RA-5 (1) (2) (5) | RA-5 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=RA-5#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=RA-5#enhancement-2) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=RA-5#enhancement-4) [(5)](http://web.nvd.nist.gov/view/800-53/control?controlName=RA-5#enhancement-5) | 1,2,3 |
| System and Services Acquisition | | | | |  |
| SA-1 | System Services Acquisition Policy and Procedures | SA-1 | SA-1 | SA-1 | 3 |
| SA-2 | Allocation of Resources | SA-2 | SA-2 | SA-2 | 1 |
| SA-3 | System Development Life Cycle | SA-3 | SA-3 | SA-3 | 1, 2, 3 |
| SA-4 | Acquisition Process | SA-4 (10) | SA-4 (1) (2) (9) (10) | SA-4 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SA-4#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=SA-4#enhancement-2) [(9)](http://web.nvd.nist.gov/view/800-53/control?controlName=SA-4#enhancement-4) (10) | 3 |
| SA-5 | Information System Documentation | SA-5 | SA-5 | SA-5 | 3 |
| SA-8 | Security Engineering Principles | Not Selected | SA-8 | SA-8 | 3 |
| SA-9 | External Information System Services | SA-9 | SA-9 (2) | SA-9 (2) | 3 |
| SA-10 | Developer Configuration Management | Not Selected | SA-10 | SA-10 | 3 |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | SA-11 | SA-11 | 3 |
| SA-12 | Supply Chain Protection | Not Selected | Not Selected | SA-12 | 3 |
| SA-15 | Development Process, Standards, and Tools | Not Selected | Not Selected | SA-15 | 3 |
| SA-16 | Developer-Provided Training | Not Selected | Not Selected | SA-16 | 3 |
| SA-17 | Developer Security Architecture and Design | Not Selected | Not Selected | SA-17 | 3 |
| System and Communications Protection | | | | |  |
| SC-1 | System and Communications Protection Policy and Procedures | SC-1 | SC-1 | SC-1 | 3 |
| SC-2 | Application Partitioning | Not Selected | SC-2 | SC-2 | 1 |
| SC-3 | Security Function Isolation | Not Selected | Not Selected | SC-3 | 1 |
| SC-4 | Information in Shared Resources | Not Selected | SC-4 | SC-4 | 1 |
| SC-5 | Denial of Service Protection | SC-5 | SC-5 | SC-5 | 1, 2, 3 |
| SC-7 | Boundary Protection | SC-7 | SC-7 (3) (4) (5) (7) | SC-7 [(3)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-7#enhancement-3) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-7#enhancement-4) [(5)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-7#enhancement-5) [(7)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-7#enhancement-7) [(8)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-7#enhancement-8) (18) (21) | 1, 2, 3 |
| SC-8 | Transmission Confidentiality and Integrity | Not Selected | SC-8 (1) | SC-8 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-8#enhancement-1) | 1, 2, 3 |
| SC-10 | Network Disconnect | Not Selected | SC-10 | SC-10 | 1 |
| SC-12 | Cryptographic Key Establishment and Management | SC-12 | SC-12 | SC-12 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SC-12#enhancement-1) | 1 |
| SC-13 | Cryptographic Protection | SC-13 | SC-13 | SC-13 | 1 |
| SC-15 | Collaborative Computing Devices | SC-15 | SC-15 | SC-15 | 1 |
| SC-17 | Public Key Infrastructure Certificates | Not Selected | SC-17 | SC-17 | 1 |
| SC-18 | Mobile Code | Not Selected | SC-18 | SC-18 | 1 |
| SC-19 | Voice Over Internet Protocol | Not Selected | SC-19 | SC-19 | 1 |
| SC-20 | Secure Name/Address Resolution Service (Authoritative Source) | SC-20 | SC-20 | SC-20 | 1 |
| SC-21 | Secure Name/Address Resolution Service (Recursive or Caching Resolver) | SC-21 | SC-21 | SC-21 | 1 |
| SC-22 | Architecture and Provisioning for Name/Address Resolution Service | SC-22 | SC-22 | SC-22 | 1 |
| SC-23 | Session Authenticity | Not Selected | SC-23 | SC-23 | 1 |
| SC-24 | Fail in Known State | Not Selected | Not Selected | SC-24 | 1 |
| SC-28 | Protection of Information at Rest | Not Selected | SC-28 | SC-28 | 1 |
| SC-39 | Process Isolation | SC-39 | SC-39 | SC-39 | 1 |
| System and Information Integrity | | | | |  |
| SI-1 | System and Information Integrity Policy and Procedures | SI-1 | SI-1 | SI-1 | 3 |
| SI-2 | Flaw Remediation | SI-2 | SI-2 (2) | SI-2 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-2#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-2#enhancement-2) | 1, 2, 3 |
| SI-3 | Malicious Code Protection | SI-3 | SI-3 (1) (2) | SI-3 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-3#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-3#enhancement-2) | 1, 2, 3 |
| SI-4 | Information System Monitoring | SI-4 | SI-4 (2) (4) (5) | SI-4 [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-4#enhancement-2) [(4)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-4#enhancement-4) [(5)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-4#enhancement-5) | 3 |
| SI-5 | Security Alerts, Advisories, and Directives | SI-5 | SI-5 | SI-5 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-5#enhancement-1) | 3 |
| SI-6 | Security Function Verification | Not Selected | Not Selected | SI-6 | 3 |
| SI-7 | Software, Firmware, and Information Integrity | Not Selected | SI-7 (1) (7) | SI-7 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-7#enhancement-1) [(2)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-7#enhancement-2) (5) (7) (14) | 3 |
| SI-8 | Spam Protection | Not Selected | SI-8 (1) (2) | SI-8 [(1)](http://web.nvd.nist.gov/view/800-53/control?controlName=SI-8#enhancement-1) (2) | 3 |
| SI-10 | Information Input Validation | Not Selected | SI-10 | SI-10 | 3 |
| SI-11 | Error Handling | Not Selected | SI-11 | SI-11 | 3 |
| SI-12 | Information Handling and Retention | SI-12 | SI-12 | SI-12 | 3 |
| SI-16 | Memory Protection | Not Selected | SI-16 | SI-16 | 3 |

Appendix B. Applicable Laws and Regulations

The following laws and regulations apply to the information system:

* Federal Information Security Modernization Act (FISMA) of 2014
* Management of Federal Information Resources [OMB Circular A-130]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]
* Privacy Act of 1974 as amended [5 USC 552a]
* E-Authentication Guidance for Federal Agencies [OMB M-04-04]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Internal Control Systems [OMB Circular A-123]
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
* Records Management by Federal Agencies [44 USC 31]
* Health Insurance Portability and Accountability Act (HIPAA) Security Rule of 1996 [45 CFR Parts 160 and 164]

The following standards and guidance apply to the information system:

* Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [NIST SP 800-37, Revision 2]
* Security and Privacy Controls for Federal Information Systems and Organizations [NIST SP 800-53, Revision 4]
* Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans [NIST SP 800-53A, Revision 4]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1: Volume 1]; Appendices [NISP SP 800-60, Revision 1: Volume 2]
* Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Conducting Risk Assessments [NIST SP 800-30, Revision 1]
* Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
* Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]
* Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]

Appendix C. Acronyms

| **Acronym** | **Definition** |
| --- | --- |
| AC | Access Control |
| AO | Authorizing Official |
| AT | Security Awareness and Training (Security Control) |
| ATO | Authorization to Operate |
| AU | Audit and Accountability (Security Control) |
| CA | Security Assessment And Authorization (Security Control) |
| CISO | Chief Information Security Officer |
| CM | Configuration Management (Security Control) |
| CNTL | Control |
| CP | Contingency Planning (Security Control) |
| CPIC | Capital Planning and Investment Control |
| CUI | Controlled Unclassified Information |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| GSS | General Support System |
| HEAR | HHS Enterprise Architecture Repository |
| HHS | Health and Human Services |
| HSPD | Homeland Security Presidential Directive |
| IA | Identification and Authentication (Security Control) |
| IHS | Indian Health Service |
| IR | Incident Response (Security Control) |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| MA | Maintenance (Security Control) |
| MOD | Moderate |
| MP | Media Access (Security Control) |
| NISP | National Information Assurance partnership |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PE | Physical and Environmental Protection (Security Control) |
| PIV | Personal Identity Verification |
| PL | Planning (Security Control) |
| POC | Point of Contact |
| PS | Personnel Security (Security Control) |
| R&C | Risk and Compliance |
| RA | Risk Assessment (Security Control) |
| RMF | Risk Management Framework |
| SA | System and Services Acquisition (Security Control) |
| SA&A | Security Assessment & Authorization |
| SAP | Security Assessment Plan |
| SAR | Security Assessment Report |
| SC | System and Communications (Security Control) |
| SI | System and Information Integrity (Security Control) |
| SP | Special Publication |
| SSP | System Security Plan |
| ST&E | Security Test and Evaluation |
| USC | United States Code |
| UUID | Universal Unique Identifier |
| VOIP | Voice Over Internet Protocol |
| WMI | Windows Management Instrumentation |