# Guide for Developing Security Plans for Federal Information Systems

**NIST**

**National Institute of Standards and Technology**

Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

# INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

*February 2006*

U.S. Department of Commerce
*Carlos M.Gutierrez, Secretary*

National Institute of Standards and Technology
*William Jeffrey, Director*

## Reports on Information Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology promotes the United States economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national-security-related information in federal information systems. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

# Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

# Acknowledgements

# Table of Contents

## Executive Summary

The objective of system security planning is to improve protection of information system resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and" Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA).

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer (SAISO). Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

In order for the plans to adequately reflect the protection of the resources, a senior management official must authorize a system to operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the system security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and the plan of actions and milestones. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur whenever there is a significant change in processing, but at least every three years.

# 1. Introduction

Today's rapidly changing technical environment requires federal agencies to adopt a minimum set of security controls to protect their information and information systems. Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies the minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. NIST SP 800-53 contains the management, operational, and technical safeguards or countermeasures prescribed for an information system.  The controls selected or planned must be documented in a system security plan.  This document provides guidance for federal agencies for developing system security plans for federal information systems.

## 1.1 Background

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. System security planning is an important activity that supports the system development life cycle (SDLC) and should be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system. The system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.  The plan also may reference other key security-related documents for the information system such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, security configuration checklists, and system interconnection agreements as appropriate.

## 1.2 Target Audience

Program managers, system owners, and security personnel in the organization must understand the system security planning process. In addition, users of the information system and those responsible for defining system requirements should be familiar with the system security planning process. Those responsible for implementing and managing information systems must participate in addressing security controls to be applied to their systems. This guidance provides basic information on how to prepare a system security plan and is designed to be adaptable in a variety of organizational structures and used as reference by those having assigned responsibility for activity related to security planning.

## 1.3 Organization of Document

This publication introduces a set of activities and concepts to develop an information system security plan. A brief description of its contents follows:

- *Chapter 1* includes background information relevant to the system security planning process, target audience, information on FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, a discussion of the various categories of information systems, identification of related NIST publications, and a description of the roles and responsibilities related to the development of system security plans.
- *Chapter 2* discusses how agencies should analyze their information system inventories in the process of establishing system boundaries. It also discusses identification of common security controls and scoping guidance.
- *Chapter 3* takes the reader through the steps of system security plan development.
- *Appendix A* provides a system security plan template.
- *Appendix B* provides a glossary of terms and definitions.
- *Appendix C* includes references that support this publication.

## 1.4 Systems Inventory and Federal Information Processing Standards (FIPS 199)

FISMA requires that agencies have in place an information systems inventory. All information systems in the inventory should be categorized using FIPS 199 as a first step in the system security planning activity.

FIPS 199 is the mandatory standard to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to impact. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

## 1.5 Major Applications, General Support Systems, and Minor Applications

All information systems must be covered by a system security plan and labeled as a major application[1] or general support system.[2]   Specific system security plans for minor

---

[1] OMB Circular A-130, Appendix III, defines major application as 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.
[2] OMB Circular A-130, Appendix III, defines general support system as 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.

applications[3] are not required because the security controls for those applications are typically provided by the general support system or major application in which they operate. In those cases where the minor application is not connected to a major application or general support system, the minor application should be briefly described in a general support system plan that has either a common physical location or is supported by the same organization. Additional information is provided in Chapter 2.

## 1.6 Other Related NIST Publications

In order to develop the system security plan, it is necessary to be familiar with NIST security standards and guidelines. It is essential that users of this publication understand the requirements and methodology for information system categorization as described in NIST FIPS 199 as well as the requirements for addressing minimum security controls for a given system as described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* and FIPS 200, *Minimum Security Requirements for Federal information and Information System.*

Other key NIST publications directly supporting the preparation of the security plan are NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.* All documents can be obtained from the NIST Computer Security Resource Center website at: http://csrc.nist.gov/.

## 1.7 System Security Plan Responsibilities

Agencies should develop policy on the system security planning process. System security plans are living documents that require periodic review, modification, and plans of action and milestones for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls. In addition, procedures should require that system security plans be developed and reviewed prior to proceeding with the security certification and accreditation process for the system.

During the security certification and accreditation process, the system security plan is analyzed, updated, and accepted. The certification agent confirms that the security controls described in the system security plan are consistent with the FIPS 199 security category determined for the information system, and that the threat and vulnerability identification and initial risk determination are identified and documented in the system security plan, risk assessment, or equivalent document. The results of a security certification are used to reassess the risks, develop the plan of action and milestones (POA&Ms) which are required to track remedial actions, and update the system security plan, thus providing the factual basis for an authorizing official to render a security

---

[3] NIST Special Publication 800-37 defines a minor application as 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.

accreditation decision. For additional information on the certification and accreditation process, see NIST SP 800-37. Figure 1, depicts the key inputs/outputs into the security planning process.
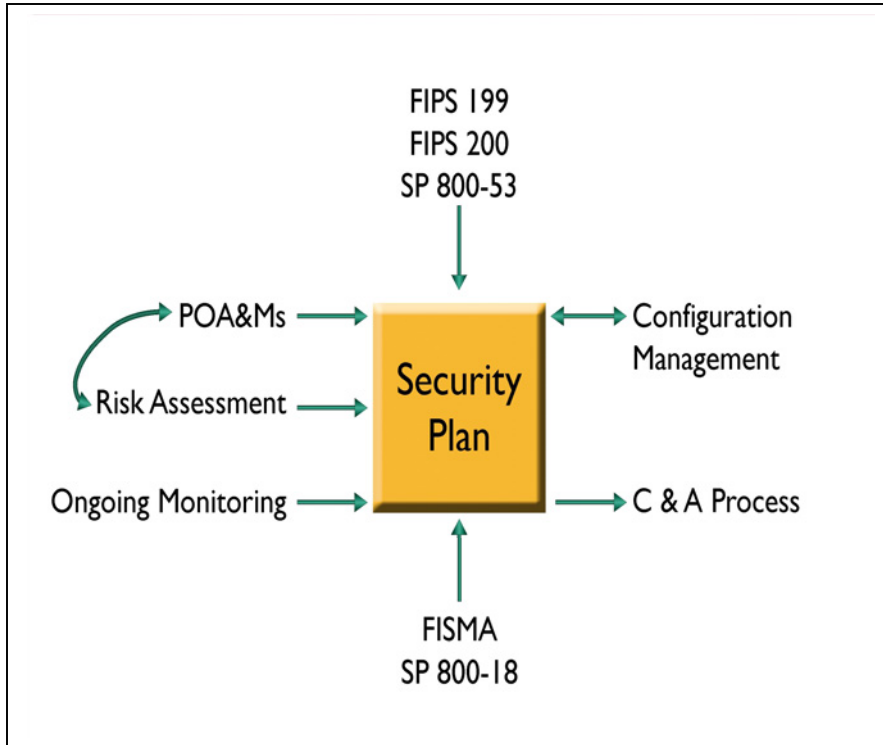


**Figure 1: Security Planning Process Inputs/Outputs**

The roles and responsibilities in this section are specific to information system security planning. Recognizing that agencies have widely varying missions and organizational structures, there may be differences in naming conventions for security planning-related roles and how the associated responsibilities are allocated among agency personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles[4]).

### 1.7.1 Chief Information Officer

The Chief Information Officer (CIO)[5] is the agency official responsible for developing and maintaining an agency-wide information security program and has the following responsibilities for system security planning:

- Designates a senior agency information security officer (SAISO) who shall carry out the CIO's responsibilities for system security planning,

---

[4] Caution should be exercised when one individual fills multiple roles in the security planning process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

[5] When an agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

- Develops and maintains information security policies, procedures, and control techniques to address system security planning,

- Manages the identification, implementation, and assessment of common security controls,

- Ensures that personnel with significant responsibilities for system security plans are trained,

- Assists senior agency officials with their responsibilities for system security plans, and

- Identifies and coordinates common security controls for the agency.

### 1.7.2 Information System Owner

The information system owner[6] is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The information system owner has the following responsibilities related to system security plans:

- Develops the system security plan in coordination with information owners, the system administrator, the information system security officer, the senior agency information security officer, and functional "end users,"

- Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,

- Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),

- Updates the system security plan whenever a significant change occurs, and

- Assists in the identification, implementation, and assessment of the common security controls.

### 1.7.3 Information Owner

The information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner has the following responsibilities related to system security plans:

---

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

- Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),[7]

- Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,

- Decides who has access to the information system and with what types of privileges or access rights, and

- Assists in the identification and assessment of the common security controls where the information resides.

### 1.7.4 Senior Agency Information Security Officer (SAISO)

The senior agency information security officer is the agency official responsible for serving as the CIO's primary liaison to the agency's information system owners and information system security officers. The SAISO has the following responsibilities related to system security plans:

- Carries out the CIO's responsibilities for system security planning,

- Coordinates the development, review, and acceptance of system security plans with information system owners, information system security officers, and the authorizing official,

- Coordinates the identification, implementation, and assessment of the common security controls, and

- Possesses professional qualifications, including training and experience, required to develop and review system security plans.

### 1.7.5 Information System Security Officer

The information system security officer is the agency official assigned responsibility by the SAISO, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. The information system security officer has the following responsibilities related to system security plans:

- Assists the senior agency information security officer in the identification, implementation, and assessment of the common security controls, and

---

[7] The information owner retains that responsibility even when the data/information are shared with other organizations.

- Plays an active role in developing and updating the system security plan as well as coordinating with the information system owner any changes to the system and assessing the security impact of those changes.

### *1.7.6 Authorizing Official*

The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.[8]  The authorizing official has the following responsibilities related to system security plans:

- Approves system security plans,

- Authorizes operation of an information system,

- Issues an interim authorization to operate the information system under specific terms and conditions, or

- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

### 1.8 Rules of Behavior

The rules of behavior, which are required in OMB Circular A-130, Appendix III, and is a security control contained in NIST SP 800-53, should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system.  It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior.  Electronic signatures are acceptable for use in acknowledging the rules of behavior.

Figure 2 lists examples from OMB Circular A-130 Appendix III of what should be covered in typical rules of behavior. These are examples only and agencies have flexibility in the detail and contents. When developing the rules of behavior, keep in mind that the intent is to make all users accountable for their actions by acknowledging that they have read, understand, and agree to abide by the rules of behavior. The rules should not be a complete copy of the security policy or procedures guide, but rather cover, at a high level, some of the controls described in the following Figure.

---

[8] In some agencies, the senior official and the Chief Information Officer may be co-authorizing officials.  In this situation, the senior official approves the operation of the information system prior to the Chief Information Officer.

---

**Examples of Controls Contained in Rules of Behavior**

- Delineate responsibilities, expected use of system, and behavior of all users.
- Describe appropriate limits on interconnections.
- Define service provisions and restoration priorities.
- Describe consequences of behavior not consistent with rules.
- Covers the following topics:
    o Work at home
    o Dial-in access
    o Connection to the Internet
    o Use of copyrighted work
    o Unofficial use of government equipment
    o Assignment and limitations of system privileges and individual accountability
    o Password usage
    o Searching databases and divulging information.

**Figure 2: Rules of Behavior Examples**

**1.9 System Security Plan Approval**

Organizational policy should clearly define who is responsible for system security plan approval and procedures developed for plan submission, including any special memorandum language or other documentation required by the agency. Prior to the certification and accreditation process, the designated Authorizing Official, independent from the system owner, typically approves the plan.

## 2. System Boundary Analysis and Security Controls

Before the system security plan can be developed, the information system and the information resident within that system must be categorized based on a FIPS 199 impact analysis. Then a determination can be made as to which systems in the inventory can be logically grouped into major applications or general support systems. The FIPS 199 impact levels must be considered when the system boundaries are drawn and when selecting the initial set of security controls (i.e., control baseline). The baseline security controls can then be tailored based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances. Common security controls, which is one of the tailoring considerations, must be identified prior to system security plan preparation in order to identity those controls covered at the agency level, which are not system-specific. These common security controls can then be incorporated into the system security plan by reference.

### 2.1 System Boundaries

The process of uniquely assigning information resources[9] to an information system defines the security boundary for that system. Agencies have great flexibility in determining what constitutes an information system (i.e., major application or general support system). If a set of information resources is identified as an information system, the resources should generally be under the same direct management control. Direct management control[10] does not necessarily imply that there is no intervening management. It is also possible for an information system to contain multiple *subsystems*.

A subsystem is a major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. Subsystems typically fall under the same management authority and are included within a single system security plan. Figure 3 depicts a general support system with three subsystems.

In addition to the consideration of direct management control, it may be helpful for agencies to consider if the information resources being identified as an information system:

- Have the same function or mission objective and essentially the same operating characteristics and security needs, and

---

[9] Information resources consist of information and related resources, such as personnel, equipment, funds, and information technology.

[10] Direct management control typically involves budgetary, programmatic, or operational authority and associated responsibility. For new information systems, management control can be interpreted as having budgetary/programmatic authority and responsibility for the development and deployment of the information systems. For information systems currently in the federal inventory, management control can be interpreted as having budgetary/operational authority for the day-to-day operations and maintenance of the information systems.

- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).



**AGENCY GENERAL SUPPORT SYSTEM**
**FIPS 199 High Impact**

**LOCAL AREA NETWORK ALPHA**
**FIPS 199 High Impact**

**SYSTEM GUARD**
**FIPS 199 High Impact**

**LOCAL AREA NETWORK BRAVO**
**FIPS 199 Moderate Impact**

Subsystem Boundary

Subsystem Boundary

Subsystem Boundary

General Support System Boundary

- One system security plan reflects information system decomposition with adequate security controls assigned to each subsystem component.

**Figure 3:  Decomposition of large and complex information systems**

While the above considerations may be useful to agencies in determining information system boundaries for purposes of security accreditation, they should not be viewed as limiting the agency's flexibility in establishing boundaries that promote effective information security within the available resources of the agency.  Authorizing officials and senior agency information security officers should consult with prospective information system owners when establishing information system boundaries.  The process of establishing boundaries for agency information systems and the associated security implications, is an agency-level activity that should include careful negotiation among all key participants—taking into account the mission/business requirements of the agency, the technical considerations with respect to information security, and the programmatic costs to the agency.

FIPS 199 defines security categories for information systems based on potential impact on organizations, assets, or individuals should there be a breach of security—that is, a loss of confidentiality, integrity, or availability.  FIPS 199 security categories can play an important part in defining information system boundaries by partitioning the agency's information systems according to the criticality or sensitivity of the information and information systems and the importance of those systems in accomplishing the agency's mission.  This is particularly important when there are various FIPS 199 impact levels contained in one information system. The FIPS 199 requirement to secure an information

system to the high watermark or highest impact level must be applied when grouping minor applications/subsystems with varying FIPS 199 impact levels into a single general support system or major application unless there is adequate boundary protection, e.g., firewalls and encryption, around those subsystems or applications with the highest impact level. Additionally, there must be assurance that the shared resources, i.e., networks, communications, and physical access within the whole general support system or major application, are protected adequately for the highest impact level. Having the ability to isolate the high impact systems will not only result in more secure systems, but will also reduce the amount of resources required to secure many applications/systems that do not require that level of security. NIST SP 800-53 provides three security control baselines, i.e., low, moderate, and high, that are associated with the three FIPS 199 impact levels; as the impact level increases, so do the minimum assurance requirements. For reporting purposes, i.e., FISMA annual report, when an information system has varying FIPS 199 impact levels, that system is categorized at the highest impact level on that information system.

## 2.2 Major Applications

All federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, store, or transmit, or because of their criticality to the agency's mission, require special management oversight. These applications are major applications. A major application is expected to have a FIPS 199 impact level of moderate or high. OMB Circular A-130 defines a "major information system" as an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. Major applications are by definition major information systems.

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific, mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel). If a system is defined as a major application and the application is run on another organization's general support system, the major application owner is responsible for acceptance of risk and in addition:

- Notifies the general support system owner that the application is critical and provides specific security requirements;

- Provides a copy of the major application's system security plan to the operator of the general support system;

- Requests a copy of the system security plan of the general support system and ensures that it provides adequate protection for the application and information; and

- Includes a reference to the general support system security plan in the major application system security plan.

## 2.3 General Support Systems

A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example[11], can be a:

- LAN including smart terminals that support a branch office;
- Backbone (e.g., agency-wide);
- Communications network;
- Agency data processing center including its operating system and utilities,
- Tactical radio network; or
- Shared information processing service facility

A general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization depending on the criticality or sensitivity of the system and any major applications the general support system is supporting. A general support system is considered a major information system when special management attention is required, there are high development, operating, or maintenance costs; and the system/information has a significant role in the administration of agency programs. When the general support system is a major information system, the system's FIPS 199 impact level is either moderate or high.

A major application can be hosted on a general support system. The general support system plan should reference the major application system security plan.

## 2.4 Minor Applications

Agencies are expected to exercise management judgment in determining which of their applications are minor applications and to ensure that the security requirements of minor applications are addressed as part of the system security plan for the applicable general support systems or, in some cases, the applicable major application. It is very common that a minor application may have a majority of its security controls provided by the general support system or major application on which it resides. If this is the case, the information system owner of the general support system or major application is the information system owner for the minor application and is responsible for developing the

---

[11] The example provided is a small sampling of general support systems; it is not a definitive list.

system security plan. The additional security controls specific to the minor application should be documented in the system security plan as an appendix or paragraph. The minor application owner (often the same as information owner) may develop the appendix or paragraph describing the additional controls. The complete general support system or major application system security plan should be shared with the information owner.

The minor application can have a FIPS 199 security category of low or moderate. However, if the minor application resides on a system that does not have adequate boundary protection, the minor application must implement the minimum baseline controls required by the host or interconnected system.

## 2.5 Security Controls

FIPS 200 provides seventeen minimum security requirements for federal information and information systems. The requirements represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity, and availability of federal information and information systems. An agency must meet the minimum security requirements in this standard by applying security controls selected in accordance with NIST SP 800-53 and the designated impact levels of the information systems. An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include: (i) the application of scoping guidance; (ii) the specification of compensating controls; and (iii) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities.

### 2.5.1 Scoping Guidance

Scoping guidance provides an agency with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines defined in NIST SP 800-53. Several considerations described below can potentially impact how the baseline security controls are applied by the agency. System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made. The application of scoping guidance must be reviewed and approved by the authorizing official for the information system.

*Technology-related considerations—*

- Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) will only be applicable if those technologies are employed or are required to be employed within the information system.

- Security controls will only be applicable to those components of the information system that typically provide the security capability addressed by the minimum security requirements.

- Security controls that can be either explicitly or implicitly supported by automated mechanisms will not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available or technically feasible, compensating security controls, implemented through non-automated mechanisms or procedures, will be used to satisfy minimum security requirements.

*Common security control-related considerations—*

- Security controls designated by the agency as common controls will, in most cases, be managed by an organizational entity other than the information system owner. Every control in a security control baseline must be addressed either by the agency through common security controls or by the information system owner. Decisions on common control designations must not, however, affect the agency's responsibility in providing the necessary security controls required to meet the minimum security requirements for the information system. (Additional information on common controls is provided in Section 2.5.3.)

*Public access information systems-related considerations—*

- Security controls associated with public access information systems must be carefully considered and applied with discretion since some of the security controls from the specified security control baselines (e.g., personnel security controls, identification and authentication controls) may not be applicable to users accessing information systems through public interfaces.[12]

*Infrastructure-related considerations—*

- Security controls that refer to agency facilities (e.g., physical access controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) will be applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, controlled interface equipment, and communications equipment).

---

[12] For example, while the baseline security controls require identification and authentication of organizational personnel who maintain and support information systems that provide public access services, the same controls might not be required for users accessing those systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication must be required for users accessing information systems through public interfaces to access their private/personal information.

*Scalability-related considerations—*

- Security controls will be scalable by the size and complexity of the particular agency implementing the controls and the impact level of the information system. Scalability addresses the breadth and depth of security control implementation. Discretion is needed in scaling the security controls to the particular environment of use to ensure a cost-effective, risk-based approach to security control implementation.[13]

*Risk-related considerations—*

- Security controls that uniquely support the confidentiality, integrity, or availability security objectives can be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high watermark;[14] (ii) is supported by an agency's assessment of risk; and (iii) does not affect the security-relevant information within the information system.[15]

### 2.5.2 Compensating Controls

Compensating security controls are the management, operational, or technical controls employed by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Compensating security controls for an information system will be employed by an agency only under the following conditions: (i) the agency selects the compensating controls from the security control catalog in NIST SP 800-53; (ii) the agency provides a complete and convincing rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the information system; and (iii) the agency assesses and formally accepts the risk associated with employing the compensating controls in the information system. The use

---

[13] For example, a contingency plan for a large and complex organization with a moderate-impact or high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a smaller organization with a low-impact information system may be considerably shorter and contain much less implementation detail.

[14] When employing the "high watermark" concept, some of the security objectives (i.e., confidentiality, integrity, or availability) may have been increased to a higher impact level. As such, the security controls that uniquely support these security objectives will have been upgraded as well. Consequently, organizations must consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[15] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) must be distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Organizations must exercise caution in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not affect the security-relevant information within the information system.

of compensating security controls must be reviewed, documented in the system security plan, and approved by the authorizing official for the information system.

### *2.5.3 Common Security Controls*

An agency-wide view of the information security program facilitates the identification of common security controls that can be applied to one or more agency information systems. Common security controls can apply to: (i) all agency information systems; (ii) a group of information systems at a specific site (sometimes associated with the terms site certification/accreditation); or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites (sometimes associated with the terms type certification/accreditation). Common security controls, typically identified during a collaborative agency-wide process with the involvement of the CIO, SAISO, authorizing officials, information system owners, and information system security officers (and by developmental program managers in the case of common security controls for common hardware, software, and/or firmware), have the following properties:

- The development, implementation, and assessment of common security controls can be assigned to responsible agency officials or organizational elements (other than the information system owners whose systems will implement or use those common security controls); and

- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of agency information systems where those controls have been applied.

Many of the management and operational controls (e.g., contingency planning controls, incident response controls, security awareness and training controls, personnel security controls, and physical security controls) needed to protect an information system may be excellent candidates for common security control status. The objective is to reduce security costs by centrally managing the development, implementation, and assessment of the common security controls designated by the agency—and subsequently, sharing assessment results with the owners of information systems where those common security controls are applied. Security controls not designated as common controls are considered *system-specific controls* and are the responsibility of the information system owner. System security plans should clearly identify which security controls have been designated as common security controls and which controls have been designated as system-specific controls.

For efficiency in developing system security plans, common security controls should be documented once and then inserted or imported into each system security plan for the information systems within the agency. The individual responsible for implementing the common control should be listed in the security plan. Effectively maximizing the application of common controls in the system security planning process depends upon the following factors:

- The agency has developed, documented, and communicated its specific guidance on identifying common security controls;

- The agency has assigned the responsibility for coordinating common security control identification and review and obtaining consensus on the common control designations, to a management official with security program responsibilities such as the CIO or SAISO;

- System owners have been briefed on the system security planning process including use of common controls; and

- Agency experts in the common control areas identified have been consulted as part of the process.

An agency may also assign a hybrid status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an agency may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. An agency may choose, for example, to implement the CP-2 (Contingency Plan) security control as a master template for a generalized contingency plan for all agency information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an agency's common security controls. These issues are identified and described in the system security plans for the individual information systems. The SAISO, acting on behalf of the CIO, should coordinate with agency officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information system owners.

Partitioning security controls into common security controls and system-specific security controls can result in significant savings to the agency in control development and implementation costs. It can also result in a more consistent application of the security controls across the agency at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the agency level. An agency-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certifications and accreditations being conducted by an agency and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an agency takes planning, coordination, and perseverance.  If an agency is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence.  Because of the potential dependence on common security controls by many of an agency's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

# 3. Plan Development

The remainder of this document guides the reader in writing a system security plan, including logical steps which should be followed in approaching plan development, recommended structure and content, and how to maximize the use of current NIST publications to effectively support system security planning activity. There should be established agency policy on how the information system security plans are to be controlled and accessed prior to initiation of the activity.

### 3.1 System Name and Identifier

The first item listed in the system security plan is the system name and identifier. As required in OMB Circular A-11, each system should be assigned a name and unique identifier. Assignment of a unique identifier supports the agency's ability to easily collect agency information and security metrics specific to the system as well as facilitate complete traceability to all requirements related to system implementation and performance. This identifier should remain the same throughout the life of the system and be retained in audit logs related to system use.

### 3.2 System Categorization

Each system identified in the agency's system inventory must be categorized using FIPS 199. NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* provides implementation guidance in completing this activity. See Table 1 for a summary of FIPS 199 categories.

### 3.3 System Owner

A designated system owner must be identified in the system security plan for each system. This person is the key point of contact (POC) for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality. The assignment of a system owner should be documented in writing and the plan should include the following contact information:

- Name
- Title
- Agency
- Address
- Phone Number
- Email Address

| Security Objective | POTENTIAL IMPACT | | |
| --- | --- | --- | --- |
| | LOW | MODERATE | HIGH |
| **Confidentiality**<br>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.<br>[44 U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity**<br>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.<br>[44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability**<br>Ensuring timely and reliable access to and use of information.<br>[44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

**Table 1: FIPS 199 Categorization**

### 3.4 Authorizing Official

An authorizing official must be identified in the system security plan for each system. This person is the senior management official who has the authority to authorize operation (accredit) of an information system (major application or general support system) and accept the residual risk associated with the system. The assignment of the authorizing official should be in writing, and the plan must include the same contact information listed in Section 3.3.

### 3.5 Other Designated Contacts

This section should include names of other key contact personnel who can address inquiries regarding system characteristics and operation. The same information listed in Section 3.3 should be included for each person listed under this section.

### 3.6 Assignment of Security Responsibility

Within an agency, an individual must be assigned responsibility for each system. This can be accomplished in many ways. In some agencies, the overall responsibility may be delegated to the SAISO. Often, the SAISO is supported by a subnet of security officers assigned to each major component. These security officers may be authorized to address the security requirements for all systems within their domain of authority. Other models may segment this responsibility in other ways based on agency structure and responsibility. The same contact information, as listed under Section 3.3, should be provided for these individuals. Most important is that this responsibility be formalized in writing either in the employee's Position Description or by delegation Memorandum.

### 3.7 System Operational Status

Indicate one or more of the following for the system's operational status. If more than one status is selected, list which part of the system is covered under each status.

- *Operational* — the system is in production.
- *Under Development* — the system is being designed, developed, or implemented.
- *Undergoing a major modification* — the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan depending on where the system is in the security life cycle.

### 3.8 Information System Type

In this section of the plan, indicate whether the system is a major application or general support system. If the system contains minor applications, describe them in the General Description/Purpose section of the plan. If the agency has additional categories of information system types, modify the template to include the other categories.

### 3.9 General Description/Purpose

Prepare a brief description (one to three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an agency, business census data analysis, crop reporting support).

If the system is a general support system, list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's agency.

**3.10 System Environment**

Provide a brief (one to three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc. Typically, operational environments are as follows:

- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, to small businesses and small branch offices of a company.

- **Managed or Enterprise** are typically large agency systems with defined, organized suites of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.

- **Custom** environments contain systems in which the functionality and degree of security do not fit the other environments. Two typical Custom environments are **Specialized Security-Limited Functionality and Legacy**:

  -- **Specialized Security-Limited Functionality**. A Specialized Security-Limited Functionality environment contains systems and networks at high risk of attack or data exposure, with security taking precedence over functionality. It assumes systems have limited or specialized (not general purpose workstations or systems) functionality in a highly threatened environment such as an outward facing firewall or public web server or whose data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as legacy applications or interoperability with other systems. A Specialized Security-Limited Functionality environment could be a subset of another environment.

  -- **Legacy**. A Legacy environment contains older systems or applications that may use older, less-secure communication mechanisms. Other machines operating in a Legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. A Legacy environment could be a subset of a standalone or managed environment.[16]

---

[16] For a detailed explanation of system environments, see NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers*.

### 3.11 System Interconnection/Information Sharing

System interconnection is the direct connection of two or more IT systems for the purpose of sharing information resources.  System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system owners, information owners, and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and information sharing. This is essential to selecting the appropriate controls required to mitigate those vulnerabilities. An Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or Memorandum of Agreement (MOA) is needed between systems (not between workstations/desktops or publicly accessed systems) that share data that are owned or operated by different organizations. An ISA is not needed with internal agency systems if an agency manages and enforces a rigid system development life cycle, which requires approvals and sign-offs ensuring compliance with security requirements. For additional information on interconnections, see NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems.*

In this section, for *each interconnection* between systems that are owned or operated by different organizations, provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- Name of system;

- Organization;

- Type of interconnection (Internet, Dial-Up, etc.);

- Authorizations for interconnection (MOU/MOA, ISA);

- Date of agreement;

- FIPS 199 Category;

- Certification and accreditation status of system; and

- Name and title of authorizing official(s).

For agencies with numerous interconnections, a table format including the above information may be a good way to present the information.

### 3.12 Laws, Regulations, and Policies Affecting the System

List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system. General agency security requirements need

not be listed since they mandate security for all systems. Each agency should decide on the level of laws, regulations, and policies to include in the system security plan. Examples might include the Privacy Act of 1974 or a specific statute or regulation concerning the information processed (e.g., tax or census information).  If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

### 3.13 Security Control Selection

In preparation for documenting how the NIST SP 800-53 security controls for the applicable security control baseline (low-, moderate-, or high impact information systems) are implemented or planned to be implemented, the security controls contained in the baseline should be reviewed and possibly tailored.  The scoping guidelines explained in Section 2.5.1 should be used when determining the applicability or tailoring of individual controls. Additionally the controls that are common among numerous systems or within the whole agency should be identified and then documented in the plan. See Section 2.5.3 for guidance on how the common controls should be determined, documented, and coordinated. The process of selecting the appropriate security controls and applying the scoping guidelines to achieve *adequate security*[17] is a multifaceted, risk-based activity involving management and operational personnel within the agency and should be conducted before the security control portion of the plan is written.

- For *low-impact* information systems, an agency must, as a minimum, employ the security controls from the low baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

- For *moderate-impact* information systems, an agency must, as a minimum, employ the security controls from the moderate baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

- For *high-impact* information systems, an agency must, as a minimum, employ the security controls from the high baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

### 3.14 Minimum Security Controls

Now that the security controls have been selected, tailored, and the common controls identified, describe each control. The description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3)

---

[17] The Office of Management and Budget (OMB) Circular A-130, Appendix III, defines adequate security as security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

Security controls in the security control catalog (NIST SP 800-53, Appendix F) have a well-defined organization and structure. The security controls are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical[18]). Each family contains security controls related to the security function of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. Table 2 summarizes the classes and families in the security control catalog and the associated family identifiers.

| CLASS | FAMILY | IDENTIFIER |
|---|---|---|
| Management | Risk Assessment | RA |
| Management | Planning | PL |
| Management | System and Services Acquisition | SA |
| Management | Certification, Accreditation, and Security Assessments | CA |
| Operational | Personnel Security | PS |
| Operational | Physical and Environmental Protection | PE |
| Operational | Contingency Planning | CP |
| Operational | Configuration Management | CM |
| Operational | Maintenance | MA |
| Operational | System and Information Integrity | SI |
| Operational | Media Protection | MP |
| Operational | Incident Response | IR |
| Operational | Awareness and Training | AT |
| Technical | Identification and Authentication | IA |
| Technical | Access Control | AC |
| Technical | Audit and Accountability | AU |
| Technical | System and Communications Protection | SC |

**Table 2: Security Control Class, Family, and Identifier**

Security control class designations (i.e., management, operational, and technical) are defined below for clarification in preparation of system security plans.
*Management controls* focus on the management of the information system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. *Operational controls* address security methods focusing on

---

[18] Security control families in NIST SP 800-53 are associated with one of three security control classes (i.e., management, operational, technical). Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management as well.

mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. ***Technical controls*** focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

## 3.15 Completion and Approval Dates

The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. When the system is updated, a version number should be added. The system security plan should also contain the date the authorizing official or the designated approving authority approved the plan. Approval documentation, i.e., accreditation letter, approval memorandum, should be on file or attached as part of the plan.

## 3.16 Ongoing System Security Plan Maintenance

Once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system. This documentation and its correctness are critical for system certification activity. All plans should be reviewed and updated, if appropriate, at least annually. Some items to include in the review are:

- Change in information system owner;
- Change in information security representative;
- Change in system architecture;
- Change in system status;
- Additions/deletions of system interconnections;
- Change in system scope;
- Change in authorizing official; and
- Change in certification and accreditation status.

## Appendix A: Sample Information System Security Plan Template

The following sample has been provided ONLY as one example. Agencies may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that numerous agencies and information security service providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility.

## Information System Security Plan Template

**1. Information System Name/Title:**
- Unique identifier and name given to the system.

**2. Information System Categorization:**
- Identify the appropriate FIPS 199 categorization.

| | LOW | | MODERATE | | HIGH |
|---|---|---|---|---|---|

**3. Information System Owner:**
- Name, title, agency, address, email address, and phone number of person who owns the system.

**4. Authorizing Official:**
- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

**5. Other Designated Contacts:**
- List other key personnel, if applicable; include their title, address, email address, and phone number.

**6. Assignment of Security Responsibility:**
- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

**7. Information System Operational Status:**
- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

| | Operational | | Under Development | | Major Modification |
|---|---|---|---|---|---|

**8. Information System Type:**
- Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.

| | Major Application | | General Support System |
|---|---|---|---|

**9. General System Description/Purpose**
- Describe the function or purpose of the system and the information processes.

**10. System Environment**
- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

## 11. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

| System Name | Organization | Type | Agreement (ISA/MOU/MOA) | Date | FIPS 199 Category | C&A Status | Auth. Official |
|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## 12. Related Laws/Regulations/Policies

- List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

## 13. Minimum Security Controls

Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from NIST SP 800-53, then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain: 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

## 14. Information System Security Plan Completion Date: _____

- Enter the completion date of the plan.

## 15. Information System Security Plan Approval Date: _____

- Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.

# Appendix B: Glossary

COMMON TERMS AND DEFINITIONS

| | |
|---|---|
| Accreditation<br>[NIST SP 800-37] | The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. |
| Accreditation Boundary<br>[NIST SP 800-37] | All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3. |
| Accrediting Authority | See Authorizing Official. |
| Adequate Security<br>[OMB Circular A-130, Appendix III] | Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. |
| Agency | See Executive Agency. |
| Authentication | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. |
| 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. See authentication. |
| Authorize Processing | See Accreditation. |
| Authorizing Official<br>[NIST SP 800-37] | Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. |
| Availability<br>[44 U.S.C., Sec. 3542] | Ensuring timely and reliable access to and use of information. |

| Certification [NIST SP 800-37] | 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. |
|---|---|
| Certification Agent [NIST SP 800-37] | The individual, group, or organization responsible for conducting a security certification. |
| Chief Information Officer [44 U.S.C., Sec. 5125(b)] | 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. |
| Common Security Control [NIST SP 800-37] | Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied. |
| Compensating Security Controls | The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system. |
| Confidentiality [44 U.S.C., Sec. 3542] | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. |

| Configuration Control [CNSS Inst. 4009] | Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation. |
|---|---|
| Countermeasures [CNSS Inst. 4009] | Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. |
| Executive Agency [41 U.S.C., Sec. 403] | 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. |
| Federal Enterprise Architecture [FEA Program Management Office] | A business-based framework for government-wide 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. |
| Federal Information System [40 U.S.C., Sec. 11331] | An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. |
| General Support System [OMB Circular A-130, Appendix III] | 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. |
| 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. |
| Information Owner [CNSS Inst. 4009] | Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. |
| Information Resources [44 U.S.C., Sec. 3502] | Information and related resources, such as personnel, equipment, funds, and information technology. |

| Information Security [44 U.S.C., Sec. 3542] | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. |
|---|---|
| Information Security Policy [CNSS Inst. 4009] | Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. |
| Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III] | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |
| Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted] | Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |
| Information System Security Officer [CNSS Inst. 4009, Adapted] | Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. |
| Information Technology [40 U.S.C., Sec. 1401] | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. |

| | |
|---|---|
| Information Type [FIPS 199] | 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. |
| Integrity [44 U.S.C., Sec. 3542] | Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. |
| Label | See Security Label. |
| Low-Impact System | An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. |
| Major Application [OMB Circular A-130, Appendix III] | 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. 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. |
| Major Information System [OMB Circular A-130] | An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. |
| Management Controls [NIST SP 800-18] | 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. |
| Media Access Control Address | A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address. |
| 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. |
| Mobile Code | Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. |

| | |
|---|---|
| Mobile Code Technologies | Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript). |
| Moderate-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 moderate and no security objective is assigned a FIPS 199 potential impact value of high. |
| National Security Emergency Preparedness Telecommunications Services | 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. |
| National Security Information | 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. |
| National Security System [44 U.S.C., Sec. 3542] | 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. |
| Non-repudiation [CNSS Inst. 4009] | Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. |
| Operational Controls [NIST SP 800-18] | The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). |

| | |
|---|---|
| Plan of Action and Milestones [OMB Memorandum 02-01] | 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. |
| Potential Impact [FIPS 199] | The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. |
| Privacy Impact Assessment [OMB Memorandum 03-22] | 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. |
| Protective Distribution System | Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information. |
| Records | The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). |
| Remote Access | Access by users (or information systems) communicating external to an information system security perimeter. |
| Remote Maintenance | Maintenance activities conducted by individuals communicating external to an information system security perimeter. |
| Risk [NIST SP 800-30] | The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. |

| Risk Assessment [NIST SP 800-30] | The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses. |
| --- | --- |
| Risk Management [NIST SP 800-30] | The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. |
| Safeguards [CNSS Inst. 4009, Adapted] | 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. |
| Sanitization [CNSS Inst. 4009, Adapted] | Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. |
| Scoping Guidance | Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline. |
| Security Category [FIPS 199] | 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. |
| Security Controls [FIPS 199] | The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. |
| Security Control Baseline | The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. |
| Security Control Enhancements | Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. |

| Security Impact Analysis [NIST SP 800-37] | The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system. |
|---|---|
| Security Label | Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein. |
| Security Objective | Confidentiality, integrity, or availability. |
| Security Perimeter | See Accreditation Boundary. |
| Security Plan | See System Security Plan. |
| Security Requirements | Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. |
| Senior Agency Information Security Officer [44 U.S.C., Sec. 3544] | 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. |
| Spyware | Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge. |
| Subsystem | A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. |
| System | See Information System. |
| System-specific Security Control [NIST SP 800-37] | A security control for an information system that has not been designated as a common security control. |
| System Security Plan [NIST SP 800-18] | Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. |

| | |
|---|---|
| Technical Controls [NIST SP 800-18] | 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. |
| Threat [CNSS Inst. 4009, Adapted] | Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. |
| Threat Agent/Source [NIST SP 800-30] | Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability. |
| Threat Assessment [CNSS Inst. 4009] | Formal description and evaluation of threat to an information system. |
| Trusted Path | A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software. |
| User [CNSS Inst. 4009] | Individual or (system) process authorized to access an information system. |
| Vulnerability [CNSS Inst. 4009, Adapted] | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. |
| Vulnerability Assessment [CNSS Inst. 4009] | Formal description and evaluation of the vulnerabilities in an information system. |

# Appendix C: References

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.

Federal Information Processing Standards Publication 200, *Security Controls for Federal Information System*, (projected for publication February 2006).

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems,* August 2002.

National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* February 2005.

National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process,* January 2005.

National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products  -- Guidance for Checklists Users and Developers,* May 2005.

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.