

**System Security Plan**

**for**

**[System Name] ([System Acronym])**

Security Categorization: [High, Moderate, or Low]

**National Cancer Institute (NCI)**

**Version X.X**

**[MM/DD/YYYY]**

**Prepared by**

**Click or tap here to enter text.**

**FOR OFFICIAL USE ONLY**

**DOCUMENT REVISION HISTORY**

This [System Acronym] System Security Plan (SSP) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed annually. Reviews made as part of the assessment process shall also be recorded below.

This document history shall be maintained throughout the life of the document and the associated system.

| Date | Description | Version | Author |
| --- | --- | --- | --- |
| mm/dd/yyyy | Initial Document Publication | 1.0 | [System Team Member/Position] |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**SYSTEM SECURITY PLAN APPROVALS**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| [Business Owner Full Name] | Date |
| Business Owner |  |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| [Information System Owner Full Name] | Date |
| System Owner |  |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| Bruce Woodcock | Date |
| NCI Information System Security Officer |  |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| Suzanne Milliard | Date |
| Privacy Coordinator |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Table of Contents**

[1 Overview 6](#_Toc536686236)

[2 System Identification 7](#_Toc536686237)

[2.1 System Name 7](#_Toc536686238)

[2.2 General System Description and Purpose 7](#_Toc536686239)

[2.3 Security Categorization 7](#_Toc536686240)

[2.4 System Lifecycle Status 7](#_Toc536686241)

[2.5 System Security Plan Completion Date 7](#_Toc536686242)

[2.6 System Security Plan Approval Date 7](#_Toc536686243)

[2.7 System Ownership 8](#_Toc536686244)

[2.7.1 Organizational Owner 8](#_Toc536686245)

[2.7.2 NCI Authorizing Official 8](#_Toc536686246)

[2.7.3 Business Owner 8](#_Toc536686247)

[2.7.4 NCI Chief Information Officer 8](#_Toc536686248)

[2.7.5 NCI Information System Security Officer 9](#_Toc536686249)

[2.7.6 System Owner 9](#_Toc536686250)

[2.7.7 Data Owner 10](#_Toc536686251)

[2.7.8 Privacy Coordinator 10](#_Toc536686252)

[2.8 System Environment 11](#_Toc536686253)

[2.8.1 System Inventory Summary 11](#_Toc536686254)

[2.8.2 NIH Tier Mapping / System Boundary 11](#_Toc536686255)

[2.8.3 Hardware Inventory 12](#_Toc536686256)

[2.8.4 Software Inventory 12](#_Toc536686257)

[2.8.5 Network Inventory 12](#_Toc536686258)

[2.8.6 Ports, Protocols and Services 12](#_Toc536686259)

[2.8.7 System Interconnections 13](#_Toc536686260)

[3 Security and Privacy Controls 14](#_Toc536686261)

[3.1 Security Control Selection 14](#_Toc536686262)

[3.2 Privacy Control Selection 15](#_Toc536686263)

[3.3 Security Control Traceability Matrix 15](#_Toc536686264)

[3.4 Security and Privacy Control Status Summary 16](#_Toc536686265)

[Appendix A - System Environment Diagram 17](#_Toc536686266)

[Appendix B - Data Flow Diagram 18](#_Toc536686267)

[Appendix C - Security Categorization 19](#_Toc536686268)

[Appendix D - System/Document Change Records 20](#_Toc536686269)

**List of Tables**

[Table 2‑1 System Name 7](#_Toc536630245)

[Table 2‑2 Security Categorization 7](#_Toc536630246)

[Table 2‑3 System Inventory Summary 11](#_Toc536630247)

[Table 2‑4 NIH Tier Mapping / System Boundary 11](#_Toc536630248)

[Table 2‑5 Hardware Inventory 12](#_Toc536630249)

[Table 2‑6 Software Inventory 12](#_Toc536630250)

[Table 2‑7 Network Inventory 12](#_Toc536630251)

[Table 2‑8 Ports, Protocols and Services 12](#_Toc536630252)

[Table 2‑9 System Interconnections 13](#_Toc536630253)

[Table 3‑1 Controls Status Summary Table 16](#_Toc536630254)

# Overview

This plan was developed in response to the requirements of the following laws and regulations:

* Federal Information Security Modernization Act (FISMA) of 2014, P.L. 113-283: A System Security Plan (SSP) is to be developed and documented for each system consistent with guidance issued by the National Institute of Standards and Technology (NIST).
* Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource: A security plan must be developed and practiced throughout all life cycles of the agency’s information systems.
* Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems. This document defines standards for the security categorization information and information systems. System security categorization must be included in SSPs.
* Federal Information Processing Standards (FIPS) Publication (PUB) 200, Minimum Security Requirements for Federal Information and Information Systems. This document contains information regarding specifications for minimum security control requirements for Federal information and information systems. Minimum security controls must be documented in SSPs.
* NIST Special Publication (SP) 800-18 Revision 1, Guide for Developing Security Plans for Information Technology Systems. The minimum standards for a SSP are provided in this NIST document.
* NIST SP 800-53, Recommended Security Controls for Federal Information Systems: This document contains a list of security controls that are to be implemented into Federal information systems based on their FIPS 199 categorization. This document is used in conjunction with FIPS 200 to define minimum security controls, which must be documented in SSPs. This document is based on NIST SP 800-53 Rev 4, updated April 2013. Additional guidance in determining control levels is derived from NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, December 2014.

The SSP documents the current and planned controls for [System Acronym] and addresses security concerns that may affect the system’s operating environment. This SSP will be part of the Security Authorization package submitted to and approved by the Authorizing Official (AO), who will authorize or deny [System Acronym] to operate.

The format of this SSP was developed in accordance with NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Information Technology Systems and NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations.

# System Identification

## System Name

Table 2‑1 System Name

| **Unique Identifier (SBID or UUID)** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| [SBID or UUID] | [System Name] | [System Acronym] |

## General System Description and Purpose

[System Acronym] is a [System Type] (General Support System, Major Application or Minor Application).

[Add description of why the system exists and what the system does]

## Security Categorization

[System Acronym] was evaluated against FIPS 199 and NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories. The following FIPS 199 security impact ratings are outlined in the [System Acronym] Security Categorization (see Appendix C).

Table 2‑2 Security Categorization

| **Security Objective** | **Low, Moderate or High** |
| --- | --- |
| Confidentiality | [Categorization] |
| Integrity | [Categorization] |
| Availability | [Categorization] |
| **Overall** | **Moderate** |

## System Lifecycle Status

The system is currently in the Operational phase of the system development life cycle.

## System Security Plan Completion Date

Completion Date: TBD

## System Security Plan Approval Date

In accordance with OMB Circular A-130, final responsibility for determining that the plan provides for reducing risk to an acceptable level should lie with the manager whose program operations and assets are at risk. The date of the accreditation memo is the approval date of this document.

## System Ownership

### Organizational Owner

National Cancer Institute

### NCI Authorizing Official

|  |  |
| --- | --- |
| **Name** |  |
| **Office Symbol** |  |
| **Title** |  |
| **Company Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

### Business Owner

|  |  |
| --- | --- |
| **Name** |  |
| **Office Symbol** |  |
| **Title** |  |
| **Company Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

### NCI Chief Information Officer

|  |  |
| --- | --- |
| **Name** | Jeffrey Shilling |
| **Office Symbol** | CBIIT/IITOB |
| **Title** | Chief Information Officer |
| **Company Name** | National Cancer Institute |
| **Address** | 9609 Medical Center Drive, Rockville, Maryland 20850 |
| **Telephone** | 240-276-5549 |
| **Email** | Jeffrey.shilling@nih.gov |
| **Responsibility** | CIO / AO |

### NCI Information System Security Officer

|  |  |
| --- | --- |
| **Name** | Bruce Woodcock |
| **Office Symbol** | CBIIT/IITOB |
| **Title** | Information Systems Security Officer |
| **Company Name** | National Cancer Institute |
| **Address** | 9609 Medical Center Drive, Rockville, Maryland 20850 |
| **Telephone** | 240-276-5050 |
| **Email** | bruce.woodcock@nih.gov |
| **Responsibility** | ISSO |

### System Owner

|  |  |
| --- | --- |
| **Name** |  |
| **Office Symbol** |  |
| **Title** |  |
| **Company Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

### Data Owner

|  |  |
| --- | --- |
| **Name** |  |
| **Office Symbol** |  |
| **Title** |  |
| **Company Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

### Privacy Coordinator

|  |  |
| --- | --- |
| **Name** | Suzanne Milliard |
| **Office Symbol** | OD/OM/OGCR |
| **Title** | Freedom of Information/Privacy Coordinator |
| **Company Name** | National Cancer Institute |
| **Address** | 9000 Rockville Pike, Bethesda, MD 20892-2580 |
| **Telephone** | 240-781-3340 |
| **Email** | milliars@mail.nih.gov |
| **Responsibility** | Privacy Coordinator |

## System Environment

Additional information can be found in diagrams in Appendix A and Appendix B.

### System Inventory Summary

Table 2‑3 System Inventory Summary

| **IP Address (Individual or Ranges)** | **URLs and Web Servers** |
| --- | --- |
|  |  |
|  |  |
|  |  |

### NIH Tier Mapping / System Boundary

Table 2‑4 NIH Tier Mapping / System Boundary

| **NIH Tier** | **Name** | **Description** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

### Hardware Inventory

Table 2‑5 Hardware Inventory

| **Name** | **IP Address** | **Subnet** | **IP** **Range** | **Vendor** | **Product** | **Model** | **Version** | **Hostname** | **Port** | **Protocol** | **Supported Modules** | **Patch Level** | **Location** | **Description** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No inventory items defined. | | | | | | | | | | | | | | |

### Software Inventory

Table 2‑6 Software Inventory

| **Name** | **IP Address** | **Subnet** | **IP Range** | **Vendor** | **Product** | **Model** | **Version** | **Hostname** | **Port** | **Protocol** | **Supported Modules** | **Patch Level** | **Location** | **Description** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No inventory items defined. | | | | | | | | | | | | | | |

### Network Inventory

Table 2‑7 Network Inventory

| **Name** | **IP Address** | **Subnet** | **IP Range** | **Vendor** | **Product** | **Model** | **Version** | **Hostname** | **Port** | **Protocol** | **Supported Modules** | **Patch Level** | **Location** | **Description** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No inventory items defined. | | | | | | | | | | | | | | |

### Ports, Protocols and Services

Table 2‑8 Ports, Protocols and Services

| **Name** | **IP Address** | **Subnet** | **IP Range** | **Vendor** | **Product** | **Model** | **Version** | **Hostname** | **Port** | **Protocol** | **Supported Modules** | **Patch Level** | **Location** | **Description** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No inventory items defined. | | | | | | | | | | | | | | |

### System Interconnections

Table 2‑9 System Interconnections

| **System Name** | **Organization** | **Type**  **(TCP/IP, Dial-up, SNA, etc.)** | **Agreement**  **(ISA/MOU/MOA/SLA)** | **Date of Agreement** | **Security Categorization** | **Authorization Status** | **Name and Title of Authorizing Official** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No interconnections defined. | | | | | | | |

# Security and Privacy Controls

This section summarizes the management, operational and technical security and privacy control requirements for the system and shows their status (in place, planned or not applicable and type of control).

The minimum security control baseline for [System Acronym] is [High, Moderate, or Low]. The system owner may identify additional controls, if necessary, to provide the desired or required level of assurance to the system’s security.

## Security Control Selection

The [System Acronym] system must meet the Federal Information Processing Standards (FIPS) 200 minimum security requirements by selecting the appropriate security and privacy controls and assurance requirements as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 (Rev. 4). The process of selecting the appropriate security controls and assurance requirements for Department information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the agency. Security categorization of federal information and information systems, as required by FIPS 199, is the first step in the risk management process. Subsequent to the security categorization process, an agency must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in FIPS 200. The selected set of security controls must be one of three security control baselines (high, moderate, low) from NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organization*, which are associated with the designated impact level of the system determined during the security categorization process. Privacy controls are defined in Appendix J of the NIST SP 800-53 Rev. 4.

Implementation status will be noted as follows:

* **In Place**: The control is fully in place as described in NIST SP 800-53 Rev. 4.
* **Partially In Place**: Aspects of the NIST SP 800-53 Rev. 4 control are in place, but part of the control has yet to be implemented.
* **Planned**: The control is not in place and there is a planned activity to implement the control.
* **Not In Place**: Risk Mitigated with Compensating Control – The compensating control must provide the equivalent or more stringent security measures than the NIST SP 800-53 Rev. 4 control. Specify whether a waiver has been requested or obtained.
* **Not Applicable**: The control is not applicable for the [System Acronym] environment.
* **Control types will be noted as follows:**
  + **Common (Inherited)**: Controls that are facilitated agency-wide. Common security controls can apply to: (i) all agency information systems; (ii) a group of information systems at a specific site; or (iii) common information systems, subsystems, or applications deployed at multiple operational sites.
  + **System**: Controls that provide a security capability for the [System Acronym] system only.
  + **Hybrid**: Controls that are implemented in part as a common control and in part as a system-specific control, i.e. policy for a system is deemed common but the procedures implementing the policy are deemed system-specific.

## Privacy Control Selection

Per National Institutes of Health (NIH) policy, privacy controls apply to all systems, regardless of categorization. The privacy control selection included in the SCTM is directly from the latest version of the NIH InfoSec Policy Handbook.

## Security Control Traceability Matrix

Rather than the security and privacy controls being spread out over hundreds of cumbersome pages within this SSP, you will see the embedded security control traceability matrix (SCTM) Excel spreadsheet below with the instructions, control information, applicable overlays, prefilled drop-downs for control type and status, and an auto-calculating security control status table to copy-and-paste into section 3.4 below. The SCTM makes the security and privacy control implementation process much more efficient for the system team and other stakeholders involved in this process than manually entering all information in a Word document format. Please open the embedded file below and read the instructions on filling the SCTM out.

[Insert Appropriate SCTM]

[Insert -----> Object -----> Create from File -----> Browse to File Location]

[\*ensure the “Display as icon” checkbox is checked]

## Security and Privacy Control Status Summary

In the following security and privacy control status table, enter the total numbers of the control implementation statuses and control types for each control family as well as the totals at the bottom. This will serve as a quick reference snapshot security and privacy control snapshot of your system for system stakeholders. The SCTM will auto-calculate this table and associated metrics, so you can just copy and paste this table from your SCTM after you have completed the SCTM.

Table 3‑1 Controls Status Summary Table

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Control Family | In Place | Partially In Place | Planned | Not Applicable | Common | Hybrid | System Specific |
| Access Control | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Accountability, Audit, and Risk Management | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Audit and Accountability | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Authority and Purpose | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Awareness and Training | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Configuration Management | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Contingency Planning | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Data Minimization and Retention | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Data Quality and Integrity | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Identification and Authentication | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Incident Response | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Individual Participation and Redress | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Maintenance | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Media Protection | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Personnel Security | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Physical and Environmental Protection | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Planning | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Program Management | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Risk Assessment | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Security | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Security Assessment and Authorization | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| System and Communications Protection | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| System and Information Integrity | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| System and Services Acquisition | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Transparency | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Use Limitation | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Totals | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Appendix A - System Environment Diagram

The system environment diagram is a visual representation that describes the hardware/software/networking environment that the system is in.

See attached file(s).

# Appendix B - Data Flow Diagram

The data flow diagram is a visual representation that describes the information flows among components within and outside of the system.

See attached file(s).

# Appendix C - Security Categorization

The security categorization for [System Acronym] is documented within the official FIPS-199 for this system and also reflected in section 2.3. The purpose of this document is to provide a standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

See attached file(s).

# Appendix D - System/Document Change Records

Documents related to formal system changes and related security impact assessments (SIAs) go in this appendix.

See attached file(s).