

OFFICIAL USE ONLY

# DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

## *SYSTEM SECURITY PLAN (SSP) TEMPLATE*

*Version 1.0*

**April 2005**

**Final**



**[SYSTEM NAME]**

**[Organization]**

**[DATE PREPARED]**

**Prepared by:**

**Preparing Organization**

## TABLE OF CONTENTS

<b>SYSTEM SECURITY PLAN REVIEW/APPROVAL SHEET</b>	<b>iii</b>
<b>SYSTEM SECURITY PLAN REVIEW SHEET</b>	<b>iv</b>
<b>SYSTEM SECURITY PLAN CHANGE INFORMATION PAGE</b>	<b>v</b>
<b>A1 SYSTEM IDENTIFICATION</b>	<b>1</b>
A1.1 System Name/Title	1
A1.2 Responsible Organization	1
A1.3 Information Contact(s)	1
A1.4 Assignment of Security Responsibility	2
<b>A2 OPERATIONAL STATUS</b>	<b>2</b>
<b>A3 GENERAL DESCRIPTION/PURPOSE</b>	<b>3</b>
<b>A4 SYSTEM ENVIRONMENT</b>	<b>3</b>
<b>A5 SYSTEM INTERCONNECTION/INFORMATION SHARING</b>	<b>4</b>
<b>A6 SENSITIVITY OF INFORMATION HANDLED</b>	<b>5</b>
A6.1 Applicable Laws or Regulations Affecting the System	6
A6.2 General Description of Information Sensitivity	7
A6.3 Protection/Certification Requirements	12
<b>A7 RISK SUMMARY</b>	<b>13</b>
<b>B1-B5 MANAGEMENT CONTROLS</b>	<b>14</b>
B1 Risk Management	15
B2 Review of Security Controls	16
B3 Life Cycle	17
B4 Authorize Processing (C&A)	19
B5 System Security Plan	<b>Error! Bookmark not defined.</b>
<b>B6-B14 OPERATIONAL CONTROLS</b>	<b>20</b>
B6 Personnel Security	20
B7 Physical and Environmental Protection	22
B8 Production, Input/Output Controls	25
B9 Contingency Planning	25
B10 Hardware and System Software Maintenance	30
B11 Data Integrity	32
B12 Documentation	35
B13 Security Awareness, Training, and Education	36
B14 Incident Response Capability	36
<b>B15-B17 TECHNICAL CONTROLS</b>	<b>38</b>
B15 Identification and Authentication	38
B16 Logical Access Controls	39
B17 Audit Trails	43
<b>Appendix A – [SYSTEM NAME] Rules of Behavior</b>	<b>A-1</b>
<b>INDEX</b>	<b>B-1</b>

**[SYSTEM NAME]**  
**SYSTEM SECURITY PLAN REVIEW/APPROVAL SHEET**

<b>System Owner:</b>		
_____	_____	_____
<b>Name:</b>	<b>Signature</b>	<b>Date</b>

<b>Security Officer:</b>		
_____	_____	_____
<b>Name:</b>	<b>Signature</b>	<b>Date</b>

<b>Security Reviewer:</b>		
_____	_____	_____
<b>Name:</b>	<b>Signature</b>	<b>Date</b>





## INTRODUCTION

The completion of System Security Plans (SSPs) is a requirement of the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* and Public Law 100-235, the Computer Security Act of 1987. Federal agencies are required to identify each computer system that contains sensitive information, and to prepare and implement a plan for the security and privacy of these systems. The objective of system security planning is to improve protection of information technology (IT) resources. All federal systems have some level of sensitivity, and require protection as part of best management practices. The protection of a system must be documented in a system security plan.

The security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from management responsible for the system, including information owners, the system operator, the system security manager, and system administrators. The system security plan delineates responsibilities and expected behavior of all individuals who access the system.

The purpose of this security plan is to provide an overview of the security of the **System Name** and describe the controls and critical elements in place or planned for, based on NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. Each applicable security control has been identified as either in place or planned. This SSP follows guidance contained in NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems* and the Department of Housing and Urban Development *Certification and Accreditation Process Guide*, April 2005.

This plan was developed by [identify team or individual who developed the plan] under the direction of the [specify HUD manager for whom the work was performed]. This plan is based upon a review of the environment, documentation, Federal and Department of Housing and Urban Development regulations/guidance, and interviews with the information system personnel conducted between dates. In addition to this System Security Plan (SSP), [specify other security documentation developed as part of the same task; e.g., “a Risk Assessment (RA), Security Test and Evaluation (ST&E), and Plan of Action and Milestones (POA&M) have been developed under this task”].

Documented in this plan are findings that indicate that there are weaknesses in **System Name** security controls that need to be corrected. These findings are summarized as follows:

- Identify here each significant risk finding.
- Identify here each significant risk finding.
- Identify here each significant risk finding.

To permit the system to operate on the basis of minimum HUD security requirements being met, the system owner should take action to implement planned corrective actions specified in this security plan as rapidly as resources permit.

## SECTION A1 SYSTEM IDENTIFICATION

### A1.1 System Name/Title

**Discussion:** Enter the system name and acronym given to the general support system or application.

### A1.2 Responsible Organization

**Discussion:** In this section, list the organization that owns and is responsible for the data in the application. The responsible organization owns the system, the data it contains, and controls the use of the data. List the federal organizational sub-component responsible for the system. If a state or local government or contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include physical locations and addresses.

The responsible organization owns the system, the data it contains, and controls the use of the data.

**Example:** Office of Financial Management  
Office of the Secretary  
U.S. Department of Housing and Urban Development  
451 7th Street S.W.,  
Washington, DC 20410

The System is maintained by:  
Appropriate Contractor Firm  
1234 Main St  
Anywhere, USA, 12345

### A1.3 Information Contact(s)

**Discussion:** Specify the program owner, program manager and the system manager to contact for further information regarding the security plan and the system. Include their address, telephone numbers, and e-mail. List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. The contacts given should be identified as the system owner, program manager, and system manager. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

The designated person(s) have sufficient knowledge of the system to be able to provide additional information or points of contact regarding the security plan and the system, as needed.

**Example:**  
System Owner  
Jane Roe  
Director, Information Resource Management Office  
U.S. Department of Housing and Urban Development  
451 7th Street S.W.,  
Washington, DC 20410  
202-708-1234  
ima.pony@abc.hud.gov

Designated Representative  
John Doe  
Department of Housing and Urban Development  
Office of ABC  
451 7th Street S.W.,  
Washington, DC 20410  
202-708-1234  
john.doe@abc.hud.gov

## A1.4 Assignment of Security Responsibility

**Discussion:** List the Information System Security Officer (ISSO), or other person(s) responsible for the security of the system, including their address and phone number. An individual must be assigned responsibility in writing to ensure that the GSS or MA has adequate security. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system. Include the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system.

You may also want to consider sending a memorandum from the organizational manager (or equivalent) to the person (or persons) identified in the SSP as responsible for security to officially confirm their appointment. If a memorandum is done, be sure to include a signed copy with the SSP.

The designated person(s) responsible for the security of the system has been assigned responsibility in writing to ensure that the GSS or MA has adequate security and is knowledgeable of the management, operational, and technical controls used to protect the system.

**Example:**  
Information System Security Officer  
Albert Einstein  
Department of Housing and Urban Development  
Office of ABC  
451 7th Street S.W.,  
Washington, DC 20410  
202-708-1234  
albert.einstein@abc.hud.gov

## A2 OPERATIONAL STATUS

**Discussion:** Indicate whether the system is **operational, under development** (or acquisition), or **undergoing a major modification**. Include date of operation, expected implementation, or completion of modification. In this section discuss: the history of the system; the date the system became or will become operational; if the system is undergoing modification; and all other pertinent information. All milestones until operational status should be stated. If the system is about to go through a major revision, all milestones along the way should be listed as well.

**Example:** The ABC LAN is currently in the operational and maintenance phase. Updates and changes to the ABC LAN are expected throughout the fiscal year. There are currently no envisioned alterations to the ABC LAN that would severely affect its operational status during updates and changes to the

system environment. The ABC system is currently in the operational and maintenance phase of the system life cycle. The system will be undergoing major modification during the course of FY 2006, including network engineering, security engineering, and systems engineering.

### A3 GENERAL DESCRIPTION/PURPOSE

**Discussion:** Present a brief description (one to three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, and crop reporting support). Be sure to include the type(s) of information that the GSS or MA processes. 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 organization, and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements are met.

**Example:** The ABC LAN is the communication system, which is designed to facilitate the services and resources needed to support the operations of ABC's users. The ABC LAN supports the following applications:

StarrFW, Application5 & Application3.

### A4 SYSTEM ENVIRONMENT

**Discussion:** Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is rapidly implemented; The software resides on an open network used by the general public or with overseas access;
- The application is processed at a facility outside of the organization's control; or
- The general support mainframe has dial-up lines.

Describe the primary computing platform(s) used (e.g., mainframe, desktop, Local Area Network (LAN) or Wide Area Network (WAN)). Include a general description of the principal system components, including hardware, software, and communications resources. Provide server names and IP addresses. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

Specify any system components that are essential to its operation, but that are not included within the scope of the plan, and the reason that this is so (i.e., covered under another plan, etc.).

Lastly, insert the system architecture diagram in this section after the text description.

**Example:** The ABC system is housed in a government owned building in Washington, DC. The entire building is occupied by the Department of Housing and Urban Development and contractor personnel and is not open to the general public. The ABC LAN operates Microsoft NT, version 4.0, and workstations run Windows 95. The security software protecting all system resources is the built in security of Microsoft Windows NT. The ABC LAN supports all office automation applications for ABC. The ABC LAN has dial up lines from each subordinate site. Users are required to be authenticated with user ID and password before access is granted to the network. Additionally, a personal firewall and up-to-date antivirus software is installed on each user's machine prior to the laptop being issued for travel.

**[Insert System Diagram Here]**

## **A5 SYSTEM INTERCONNECTION/INFORMATION SHARING**

**Discussion:** System interconnection is the direct connection of 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 operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to affect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems. A description of the rules for interconnecting systems and for protecting shared data must be included with this security plan.

In this section, provide the following information concerning the authorization for the connection to other systems or the sharing of information:

List of interconnected systems (including Internet);

- Unique system identifiers, if appropriate;
- Name of system(s);
- Organization owning the other system(s);
- Type of interconnection (TCP/IP, Dial, SNA, etc.);
- Short discussion of major concerns or considerations in determining interconnection (do not repeat the system rules included in Section 4.3);
- Name and title of authorizing management official(s);
- Date of authorization;
- System of Record, if applicable (Privacy Act data);
- Sensitivity level of each system;

- Interaction among systems; and
- Security concerns and Rules of Behavior of the other systems that need to be considered in the protection of this system.

**Example:** The ABC LAN is interconnected with the HUD XYZ backbone for Internet and Intranet access. The ABC LAN is a level II system and the information within the ABC LAN is currently shared with other HUD activities, and other Federal agencies. MOUs dated 12 Oct 02, exist that have been approved by legal and are on file with the ISSO. The Rules of Behavior have to be read, understood, and signed by each user.

## A6 SENSITIVITY OF INFORMATION HANDLED

**Discussion:** This section provides a description of the types of information handled by the system and an analysis of the sensitivity of the information. The sensitivity of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and is one of the major factors in risk management. The description will provide information to a variety of users, including:

Analysts/programmers who will use it to help design appropriate security controls; Internal and external auditors evaluating system security measures; and managers making decisions about the reasonableness of security countermeasures. Sensitivity levels range from low to high based on the type(s) of information processed. Exhibit 1 below summarizes the sensitivity levels, while Exhibit 2 provides examples of the types of information that fall into each sensitivity category. Determine the sensitivity level of the information based on the information in Exhibits 1 and 2. Indicate the overall system sensitivity level by using the highest data sensitivity level from the table. These sensitivity levels also apply to systems under development. Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. The description must contain information on applicable laws, regulations, and policies affecting the system and a general description of sensitivity. The nature of the information sensitivity and criticality must be described in this section.

**Exhibit 1: Sensitivity Levels and Descriptions**

Sensitivity Level	Description of Sensitivity Level
High	<p><i>Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:</i></p> <ul style="list-style-type: none"> <li>• Would have an <b>IRREPARABLE IMPACT</b> on Major Application (MA) or General Support System (GSS), functions, image, or reputation, such that the catastrophic result would not be able to be repaired or set right again, or</li> <li>• Could result in <b>LOSS OF MAJOR TANGIBLE ASSETS</b> or resources, including posing a threat to human life</li> </ul>
Moderate	<p><i>Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:</i></p> <ul style="list-style-type: none"> <li>• Would have an <b>ADVERSE IMPACT</b> on MA or GSS missions, functions, image, or reputation, such that the impact would place the MA at a significant disadvantage, or</li> <li>• Could result in <b>LOSS OF SIGNIFICANT TANGIBLE ASSETS</b> or resources</li> </ul>
Low	<p><i>Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:</i></p> <ul style="list-style-type: none"> <li>• Would have a <b>MINIMAL IMPACT</b> on MA or GSS missions, functions, image, or reputation, such that the impact would result in the least possible significant unfavorable condition with a negative outcome, or</li> <li>• Could result in <b>LOSS OF SOME TANGIBLE ASSETS</b> or resources</li> </ul>

**Example:** The ABC LAN is the primary communications network that supports ABC’s users in their day-to-day operations. This network is continuously used during business and non-business hours. The confidentiality, integrity and availability of the ABC LAN is critical, i.e., ensuring that data is only received by the person that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed.

**A6.1 Applicable Laws or Regulations Affecting the System**

Discussion: List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of data/information in this specific application. The Computer Security Act of 1987, OMB Circular A-130, and general agency security requirements need not be listed since they mandate security for all systems. Each organization should decide on the level of laws, regulations, and policies to include in the security plan. Examples might include the Privacy Act 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.

See the NIST Computer Security Division’s Computer Security Resource Clearinghouse (CSRC) Web site for additional information (<http://csrc.nist.gov>). CSRC contains information on a wide variety of computer security resources, including a list of applicable laws and regulations.

- **Example:** This section shows the Federal laws, regulatory guidance, and directives that drive Department of Housing and Urban Development’s IT security program.
- Federal Information Security Management Act (FISMA) of 2002
- Computer Fraud and Abuse Act of 1986, as amended.
- Computer Security Act of 1987
- Privacy Act of 1987
- OMB Circular No. A-130, Appendix III
- Federal Information Processing Standard 199 -
- NIST SP 800-18 - Guide for Developing Security Plans for Information Technology Systems, December 1998
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems, July 2002
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems, January 2002
- NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-37 – Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
- NIST SP 800-53 – Recommended Security Controls for Federal Information Systems, February 2005
- NIST SP 800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- HUD Certification and Accreditation Process Guide, April 2005
- HUD IT System Certification and Accreditation Inventory Guide, April 2005

## A6.2 General Description of Information Sensitivity

The following table provides a general description of the information handled by the system and the need for protective measures.

### Exhibit 2: Information Categories

**Discussion:** This table should be copied from the Risk Assessment Report in its entirety. **Ensure that only those information categories applicable to the system/application are included deleting the rows that do not apply.** For each category of information describe protection requirements on the basis of its need for confidentiality, integrity, and availability. Do not rank protection requirements (i.e., “Low,” “Moderate,” “High” in this table; that is performed in Exhibit 3.

Information Category	Explanation and Examples	Protection Requirements
----------------------	--------------------------	-------------------------

Information Category	Explanation and Examples	Protection Requirements
Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
Internal administration	Information related to the internal administration of HUD. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>

Information Category	Explanation and Examples	Protection Requirements
Investigation, intelligence, Critical Element related, and security information (14 CFR PART 191.5(D))	Information related to investigations for law enforcement purposes; intelligence Critical Element related information that cannot be classified but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
Other Federal agency information	Information that is required by statute to be protected, or which has come from another Federal agency and requires release approval by the originating agency.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
New technology or controlled scientific information	Information related to new technology, scientific information that is prohibited from disclosure to certain foreign governments, or that may require an export license from the Department of State and/or the Department of Commerce.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
Mission-critical information	Information designated as critical to a HUD mission; includes vital statistics information for emergency operations.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>

Information Category	Explanation and Examples	Protection Requirements
Operational information	Information that requires protection during operations; usually time-critical information.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>
System configuration Management information	Any information pertaining to the internal operations of a network or computer system, including, but not limited to, network and device addresses, system and protocol addressing schemes implemented at HUD, network management information protocols, community strings, network information packets, etc., device and system passwords, and device and system configuration information.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>

Information Category	Explanation and Examples	Protection Requirements
Public information	Any information that is declared for public consumption by official HUD authorities. This includes information contained in press releases approved by Public Affairs or other official HUD source. It also includes Information placed on public access world-wide-web (WWW) servers.	<ul style="list-style-type: none"> <li>• Confidentiality – [describe why the confidentiality of system data needs protection]</li> <li>• Integrity – [describe why the integrity of system data needs protection]</li> <li>• Availability – [describe why the availability of the system must be safeguarded]</li> </ul>

**Example:**

Information Category	Explanation and Examples	Protection Requirements
Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).	<ul style="list-style-type: none"> <li>• Confidentiality – The system contains personal information relating to payroll processing for approximately 175 personnel.</li> <li>• Integrity – The accuracy of employee payroll transactions is based upon the integrity of personal data used by the system.</li> <li>• Availability – Non-availability of the system would result in a noticeable impact on HUD missions, functions, image, or reputation. However, the impact is diminished since operations can be resumed by manual means in degraded form for an extended period.</li> </ul>

## A6.3 Protection/Certification Requirements

The following table documents general protection and certification requirements for the system.

The purpose of this table is to establish the protection requirements for the system, and to document the level of effort that will be required to certify the system. Rank as High, Moderate, or Low, and justify the ranking for each of the three primary security concerns. Then rank the system's exposure to external threats, and for systems with High confidentiality concerns, rank the exposure to internal threats. Use FIPS 199, NIST Special Pub 800-37, and the HUD C&A Process Guide to complete this table.

**Exhibit 3: Protection/Certification Requirements**

Concern	Ranking <i>(Low-Mod-High)</i>	Justification
<b>Sensitivity</b>		
Confidentiality		
Integrity		
Availability		
<b>Certification Level of Effort</b>	<b>Select either Low, Moderate, or High according to highest sensitivity ranking from above</b>	<p><b>Delete the two that do not apply</b></p> <p><b>Low</b> = Low intensity, checklist-based, independent security review</p> <ul style="list-style-type: none"> <li>• Interview of personnel</li> <li>• Review of system-related security policies, procedures, documents</li> <li>• Observation of system operations and security controls</li> </ul> <p><b>Moderate</b> = Moderate intensity, demonstration-based, independent assessment</p> <ul style="list-style-type: none"> <li>• Functional testing</li> <li>• Regression analysis and regression testing</li> <li>• Penetration testing (optional)</li> <li>• Demonstrations to verify security control correctness and effectiveness</li> <li>• Low Certification Level verification techniques (if appropriate)</li> </ul> <p><b>High</b> = High intensity, exercised-based, independent assessment</p> <ul style="list-style-type: none"> <li>• System design analysis</li> <li>• Functional testing with coverage analysis</li> <li>• Regression analysis and regression testing</li> <li>• Penetration testing (Red Team optional)</li> <li>• Demonstrations and exercises to verify security control correctness and effectiveness</li> <li>• Low and Moderate Certification Level verification techniques (if appropriate)</li> </ul>

**EXAMPLE**

Concern	Ranking <i>(Low-Mod-High)</i>	Justification
<b>Sensitivity</b> <i>(From Table 3.1, NIST SP 800-37)</i>		
Confidentiality	Low	The consequences of unauthorized disclosure or compromise

Concern	Ranking <i>(Low-Mod-High)</i>	Justification
		of data or information in the system are generally acceptable. The loss of confidentiality could be expected to affect HUD level interests and have some negative impact on mission accomplishment.
Integrity	Moderate	The consequences of corruption or unauthorized modification of data or information in the system are only marginally acceptable. Loss of integrity could be expected to adversely affect HUD level interests, and degrade mission accomplishment.
Availability	Low	The consequences of loss or disruption of access to system resources or to data or information in the system are generally acceptable. The loss of availability could be expected to affect HUD level interests and have some negative impact on mission accomplishment.
Certification Level of Effort	Moderate	Moderate intensity, demonstration-based, independent assessment <ul style="list-style-type: none"> <li>• Functional testing</li> <li>• Regression analysis and regression testing</li> <li>• Penetration testing (optional)</li> <li>• Demonstrations to verify security control correctness and effectiveness</li> <li>• Low Certification Level verification techniques (if appropriate)</li> </ul>

## A7 RISK SUMMARY

The results of the [System Name](#) Risk Assessment indicated that the risks to system resources in the areas of Management, Operational, and Technical controls are as follows:

Summarize risk assessment findings below

- **Management Controls:** The most significant management control related risks include [summarize weaknesses in management controls here, e.g., “weaknesses in the approval of security plan and risk assessment documentation; lack of rules of behavior; and, the lack of a formal authorization to operate.”]
- **Operational Controls:** Significant operational control risks include [summarize weaknesses in operational controls here, e.g., “the lack of media controls; background screening controls; lack of documented instructions for requesting, establishing, issuing and closing user accounts; lack of periodic validation of user accounts; and, lack of restrictions on software/hardware maintenance personnel.”]
- **Technical Controls:** The most significant technical control risks include [summarize weaknesses in technical controls here, e.g., “the failure to implement a log-on banner; failure to detect unauthorized access attempts through editing; and the lack of periodic vulnerability scanning.”]

Risks in areas such as natural, environmental, human intentional and human unintentional threats were assessed. The assessment found that identified risks could be fully mitigated through the implementation of security controls specified in Table 5-1 of the [System Name](#) Risk Assessment.

**Figure 5.1**

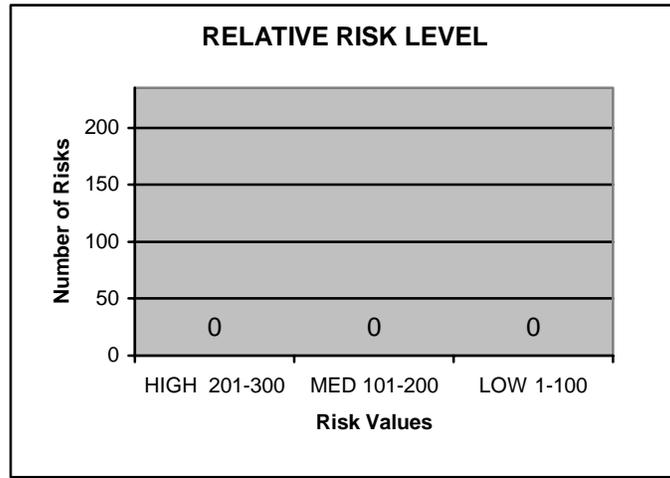


Figure 5.1 above summarizes risks identified in the [System Name] Risk Assessment. Number vulnerabilities found in System Name controls are ranked as low, medium and/or high risk. Therefore, System Name is categorized as having a low, medium or high level of risk.

## SECTION B CONTROLS IDENTIFICATION

This section documents management, operational and technical controls requirements for the system and their status as being either in place or planned in accordance with NIST SP 800-18.

For SCL-1 (Low Impact) systems the Controls Identification section will consist of the following Controls Status Summary Table and a completed Minimum Security Baseline Assessment.

**Exhibit 4: Controls Status Summary Table (SCL-1 Systems Only)**

Control Category	In Place	Planned
Risk Assessment		
Planning		
Systems and Services Acquisition		
Certification, Accreditation, and Security Assessments		
Personnel Security		
Physical and Environmental Protection		
Contingency Planning		
Configuration Management		
Maintenance		
System and Information Integrity		
Media Protection		

Incident Response		
Awareness and Training		
Identification and Authentication		
Access Controls		
Audit and Accountability		
System and Communications Protection		

For SCL-1 systems the completed *Minimum Security Baseline Assessment* here and disregard (delete) Sections B1-B17 below.

## B1-B4 MANAGEMENT CONTROLS

This section describes management controls applicable to the [System Name].

### B1 Risk Assessment (RA)

The status of risk assessment controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control  [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
<b>RA-1</b>	<b>Risk Assessment Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.			<b>A</b>
<b>RA-2</b>	<b>Security Categorization:</b> The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.			<b>A</b>
<b>RA-3</b>	<b>Risk Assessment:</b> The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.			<b>A</b>

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>RA-4</b>	<b>Risk Assessment Update:</b> The organization updates the risk assessment every three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.			<b>A</b>
<b>RA-5</b>	<b>Vulnerability Scanning:</b> Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system every six months or when significant new vulnerabilities affecting the system are identified and reported.			<b>MH</b>
<b>RA-5 (1)</b>	<b>Vulnerability Scanning:</b> Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned.			<b>H</b>
<b>RA-5 (2)</b>	<b>Vulnerability Scanning:</b> The organization updates the list of information system vulnerabilities every six months or when significant new vulnerabilities are identified and reported.			<b>H</b>

## B2 Planning (PL)

The status of security planning controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>PL-1</b>	<b>Security Planning Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.			<b>A</b>
<b>PL-2</b>	<b>System Security Plan:</b> The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.			<b>A</b>

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
PL-3	<b>System Security Plan Update:</b> The organization reviews the security plan for the information system annually and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.			A
PL-4	<b>Rules of Behavior:</b> The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.			A
PL-5	<b>Privacy Impact Assessment:</b> The organization conducts a privacy impact assessment on the information system.			A

### B3 System and Services Acquisition (SA)

The status of system and services acquisition controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
SA-1	<b>System and Services Acquisition Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.			A
SA-2	<b>Allocation of Resources:</b> The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.			A

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
SA-3	Life Cycle Support: The organization manages the information system using a system development life cycle methodology that includes information security considerations.			A
SA-4	Acquisitions: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.			A
SA-5	Information System Documentation: The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.			A
SA-5 (1)	Information System Documentation: The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.			MH
SA-5 (2)	Information System Documentation: The organization includes documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).			H
SA-6	Software Usage Restrictions: The organization complies with software usage restrictions.			A
SA-7	User Installed Software: The organization enforces explicit rules governing the downloading and installation of software by users.			A
SA-8	Security Design Principles: The organization designs and implements the information system using security engineering principles.			MH
SA-9	Outsourced Information System Services: The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.			A

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>SA-10</b>	Developer Configuration Management: The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.			<b>H</b>
<b>SA-11</b>	Developer Security Testing: The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.			<b>MH</b>

## B4 Certification, Accreditation, and Security Assessments (CA)

The status of certification, accreditation, and security assessment controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>CA-1</b>	Certification, Accreditation, and Security Assessment Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.			<b>A</b>
<b>CA-2</b>	Security Assessments: The organization conducts an assessment of the security controls in the information system annually 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.			<b>MH</b>

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>CA-3</b>	Information System Connections: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.			<b>A</b>
<b>CA-4</b>	Security Certification: The organization conducts an assessment of the security controls in the information system 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.			<b>A</b>
<b>CA-5</b>	Plan of Action and Milestones: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization’s planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.			<b>A</b>
<b>CA-6</b>	Security Accreditation: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.			<b>A</b>
<b>CA-7</b>	Continuous Monitoring: The organization monitors the security controls in the information system on an ongoing basis.			<b>A</b>

## B5-B13 OPERATIONAL CONTROLS

This section describes the level of implementation of operational controls for the [System Name].

### B5 Personnel Security (PS)

The status of personnel security controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only; RB=risk based. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
PS-1	<b>Personnel Security Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.			A
PS-2	<b>Position Categorization:</b> The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations periodically in accordance with OPM guidance.			A
PS-3	<b>Personnel Screening:</b> The organization screens individuals requiring access to organizational information and information systems before authorizing access.			A
PS-4	<b>Personnel Termination:</b> When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.			A
PS-5	<b>Personnel Transfer:</b> The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).			A
PS-6	<b>Access Agreements:</b> The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.			A
PS-7	<b>Third-Party Personnel Security:</b> The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.			A

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
PS-8	<b>Personnel Sanctions:</b> The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.			A

## B6 Physical and Environmental Protection (PE)

The status of physical and environmental protection controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
PE-1	<b>Physical and Environmental Protection Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.			A
PE-2	<b>Physical Access Authorizations:</b> The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials once a year.			A
PE-3	<b>Physical Access Control:</b> The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.			A
PE-4	<b>Access Control for Transmission Medium:</b> The organization controls physical access to information system transmission lines			RB

OFFICIAL USE ONLY

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.			
PE-5	<b>Access Control for Display Medium:</b> The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.			MH
PE-6	<b>Monitoring Physical Access:</b> The organization monitors physical access to information systems to detect and respond to incidents.			A
PE-6 (1)	<b>Monitoring Physical Access:</b> The organization monitors real-time intrusion alarms and surveillance equipment.			MH
PE-6 (2)	<b>Monitoring Physical Access:</b> The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.			H
PE-7	<b>Visitor Control:</b> The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.			A
PE-7 (1)	<b>Visitor Control:</b> The organization escorts visitors and monitors visitor activity, when required.			MH
PE-8	<b>Access Logs:</b> The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Visitor logs are reviewed at closeout, maintained on file, and available for further review for one year.			A
PE-8 (1)	<b>Access Logs:</b> The organization employs automated mechanisms to facilitate the maintenance and review of access logs.			MH
PE-9	<b>Power Equipment and Power Cabling:</b> The organization protects power equipment and power cabling for the information system from damage and destruction.			MH
PE-9 (1)	<b>Power Equipment and Power Cabling:</b> The organization employs redundant and parallel power cabling paths.			RB

OFFICIAL USE ONLY

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>PE-10</b>	<b>Emergency Shutoff:</b> For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.			<b>MH</b>
<b>PE-11</b>	<b>Emergency Power:</b> The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.			<b>MH</b>
<b>PE-11 (1)</b>	<b>Emergency Power:</b> The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.			<b>H</b>
<b>PE-11 (2)</b>	<b>Emergency Power:</b> The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.			<b>RB</b>
<b>PE-12</b>	<b>Emergency Lighting:</b> The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.			<b>A</b>
<b>PE-13</b>	<b>Fire Protection:</b> The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.			<b>A</b>
<b>PE-13 (1)</b>	<b>Fire Protection:</b> Fire suppression and detection devices/systems activate automatically in the event of a fire.			<b>MH</b>
<b>PE-13 (2)</b>	<b>Fire Protection:</b> Fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.			<b>H</b>
<b>PE-14</b>	<b>Temperature and Humidity Controls:</b> The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.			<b>A</b>
<b>PE-15</b>	<b>Water Damage Protection:</b> The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that			<b>A</b>

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	master shutoff valves are accessible, working properly, and known to key personnel.			
PE-15 (1)	<b>Water Damage Protection:</b> The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.			H
PE-16	<b>Delivery and Removal:</b> The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.			A
PE-17	<b>Alternate Work Site:</b> Individuals within the organization employ appropriate information system security controls at alternate work sites.			MH

## B7 Contingency Planning (CP)

The status of contingency planning controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
CP-1	<b>Contingency Planning Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.			A
CP-2	<b>Contingency Plan:</b> The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.			A

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
CP-2 (1)	<b>Contingency Plan:</b> The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).			MH
CP-3	<b>Contingency Training:</b> The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.			MH
CP-3 (1)	<b>Contingency Training:</b> The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.			H
CP-3 (2)	<b>Contingency Training:</b> The organization employs automated mechanisms to provide a more thorough and realistic training environment.			RB
CP-4	<b>Contingency Plan Testing:</b> The organization tests the contingency plan for the information system at least annually using to determine the plan’s effectiveness and the organization’s readiness to execute the plan. System rated as high shall be tested at the alternate processing site. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.			MH
CP-4 (1)	<b>Contingency Plan Testing:</b> The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).			MH
CP-4 (2)	<b>Contingency Plan Testing:</b> The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site’s capabilities to support contingency operations.			H
CP-4 (3)	<b>Contingency Plan Testing:</b> The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.			RB
CP-5	<b>Contingency Plan Update:</b> The organization reviews the contingency plan for the information system once per year and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or			A

OFFICIAL USE ONLY

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	testing.			
<b>CP-6</b>	<b>Alternate Storage Sites:</b> The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.			<b>MH</b>
<b>CP-6 (1)</b>	<b>Alternate Storage Sites:</b> The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.			<b>MH</b>
<b>CP-6 (2)</b>	<b>Alternate Storage Sites:</b> The alternate storage site is configured to facilitate timely and effective recovery operations.			<b>H</b>
<b>CP-6 (3)</b>	<b>Alternate Storage Sites:</b> The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.			<b>H</b>
<b>CP-7</b>	<b>Alternate Processing Sites:</b> The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within 24 hours when the primary processing capabilities are unavailable.			<b>MH</b>
<b>CP-7 (1)</b>	<b>Alternate Processing Sites:</b> The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.			<b>MH</b>
<b>CP-7 (2)</b>	<b>Alternate Processing Sites:</b> The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.			<b>MH</b>
<b>CP-7 (3)</b>	<b>Alternate Processing Sites:</b> Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.			<b>MH</b>
<b>CP-7 (4)</b>	<b>Alternate Processing Sites:</b> The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.			<b>H</b>
<b>CP-8</b>	<b>Telecommunications Services:</b> The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within 24 hours when the primary telecommunications capabilities are unavailable.			<b>MH</b>

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
CP-8 (1)	<b>Telecommunications Services:</b> Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization’s availability requirements.			MH
CP-8 (2)	<b>Telecommunications Services:</b> Alternate telecommunications services do not share a single point of failure with primary telecommunications services.			MH
CP-8 (3)	<b>Telecommunications Services:</b> Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.			H
CP-8 (4)	<b>Telecommunications Services:</b> Primary and alternate telecommunications service providers have adequate contingency plans.			H
CP-9	<b>Information System Backup:</b> The organization conducts backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.			A
CP-9 (1)	<b>Information System Backup:</b> The organization tests backup information to ensure media reliability and information integrity.			MH
CP-9 (2)	<b>Information System Backup:</b> The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.			H
CP-9 (3)	<b>Information System Backup:</b> The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.			H
CP-10	<b>Information System Recovery and Reconstitution:</b> The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system’s original state after a disruption or failure.			A
CP-10 (1)	<b>Information System Recovery and Reconstitution:</b> The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.			H

## B8 Configuration Management (CM)

The status of configuration management controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

<b>Control Number</b>	<b>Description of Control</b> <i>[Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]</i>	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>CM-1</b>	<b>Configuration Management Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.			<b>A</b>
<b>CM-2</b>	<b>Baseline Configuration:</b> The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system’s constituent components.			<b>A</b>
<b>CM-2 (1)</b>	<b>Baseline Configuration:</b> The organization updates the baseline configuration as an integral part of information system component installations.			<b>MH</b>
<b>CM-2 (2)</b>	<b>Baseline Configuration:</b> The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.			<b>H</b>
<b>CM-3</b>	<b>Configuration Change Control:</b> The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.			<b>MH</b>
<b>CM-3 (1)</b>	<b>Configuration Change Control:</b> The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.			<b>H</b>
<b>CM-4</b>	<b>Monitoring Configuration Changes:</b> The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.			<b>MH</b>

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
CM-5	<b>Access Restrictions for Change:</b> The organization enforces access restrictions associated with changes to the information system.			MH
CM-5 (1)	<b>Access Restrictions for Change:</b> The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.			H
CM-6	<b>Configuration Settings:</b> The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.			A
CM-6 (1)	<b>Configuration Settings:</b> The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.			H
CM-7	<b>Least Functionality:</b> The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of any protocol or service that is not explicitly permitted.			MH
CM-7 (1)	<b>Least Functionality:</b> The organization reviews the information system annually, to identify and eliminate unnecessary functions, ports, protocols, and/or services.			H

## B9 Maintenance (MA)

The status of maintenance controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
MA-1	<b>System Maintenance Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.			A

OFFICIAL USE ONLY

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
MA-2	<b>Periodic Maintenance:</b> The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.			A
MA-2 (1)	<b>Periodic Maintenance:</b> The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).			MH
MA-2 (2)	<b>Periodic Maintenance:</b> The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.			H
MA-3	<b>Maintenance Tools:</b> The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.			MH
MA-3 (1)	<b>Maintenance Tools:</b> The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.			H
MA-3 (2)	<b>Maintenance Tools:</b> The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.			H
MA-3 (3)	<b>Maintenance Tools:</b> The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.			H
MA-3 (4)	<b>Maintenance Tools:</b> The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.			RB
MA-4	<b>Remote Maintenance:</b> The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.			A

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
MA-4 (1)	<b>Remote Maintenance:</b> The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.			H
MA-4 (2)	<b>Remote Maintenance:</b> The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.			H
MA-4 (3)	<b>Remote Maintenance:</b> Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.			H
MA-5	<b>Maintenance Personnel:</b> The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.			A
MA-6	<b>Timely Maintenance:</b> The organization obtains maintenance support and spare parts within 48 hours of failure.			MH

## B10 System and Information Integrity (SI)

The status of system and information integrity controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
SI-1	<b>System and Information Integrity Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.			A
SI-2	<b>Flaw Remediation:</b> The organization identifies, reports, and corrects information system flaws.			A

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
SI-2 (1)	<b>Flaw Remediation:</b> The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.			RB
SI-2 (2)	<b>Flaw Remediation:</b> The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.			RB
SI-3	<b>Malicious Code Protection:</b> The information system implements malicious code protection that includes a capability for automatic updates.			A
SI-3 (1)	<b>Malicious Code Protection:</b> The organization centrally manages virus protection mechanisms.			MH
SI-3 (2)	<b>Malicious Code Protection:</b> The information system automatically updates virus protection mechanisms.			H
SI-4	<b>Intrusion Detection Tools and Techniques:</b> The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.			MH
SI-4 (1)	<b>Intrusion Detection Tools and Techniques:</b> The organization networks individual intrusion detection tools into a system-wide intrusion detection system using common protocols.			RB
SI-4 (2)	<b>Intrusion Detection Tools and Techniques:</b> The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks.			RB
SI-4 (3)	<b>Intrusion Detection Tools and Techniques:</b> The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.			RB
SI-4 (4)	<b>Intrusion Detection Tools and Techniques:</b> The information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).			RB
SI-5	<b>Security Alerts and Advisories:</b> The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.			A

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
<b>SI-5 (1)</b>	<b>Security Alerts and Advisories:</b> The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.			<b>RB</b>
<b>SI-6</b>	<b>Security Functionality Verification:</b> The information system verifies the correct operation of security functions periodically every year and notifies system administrator when anomalies are discovered.			<b>MH</b>
<b>SI-6 (1)</b>	<b>Security Functionality Verification:</b> The organization employs automated mechanisms to provide notification of failed security tests.			<b>H</b>
<b>SI-6 (2)</b>	<b>Security Functionality Verification:</b> The organization employs automated mechanisms to support management of distributed security testing.			<b>RB</b>
<b>SI-7</b>	<b>Software and Information Integrity:</b> The information system detects and protects against unauthorized changes to software and information.			<b>H</b>
<b>SI-8</b>	<b>Spam and Spyware Protection:</b> The information system implements spam and spyware protection.			<b>MH</b>
<b>SI-8 (1)</b>	<b>Spam and Spyware Protection:</b> The organization centrally manages spam and spyware protection mechanisms.			<b>H</b>
<b>SI-8 (2)</b>	<b>Spam and Spyware Protection:</b> The information system automatically updates spam and spyware protection mechanisms.			<b>RB</b>
<b>SI-9</b>	<b>Information Input Restrictions:</b> The organization restricts the information input to the information system to authorized personnel only.			<b>MH</b>
<b>SI-10</b>	<b>Information Input Accuracy, Completeness, and Validity:</b> The information system checks information inputs for accuracy, completeness, and validity.			<b>MH</b>
<b>SI-11</b>	<b>Error Handling:</b> The information system identifies and handles error conditions in an expeditious manner.			<b>MH</b>
<b>SI-12</b>	<b>Output Handling and Retention:</b> The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.			<b>MH</b>

## B11 Media Protection (MP)

The status of media protection controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
MP-1	<b>Media Protection Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.			A
MP-2	<b>Media Access:</b> The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.			A
MP-2 (1)	<b>Media Access:</b> Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.			H
MP-3	<b>Media Labeling:</b> The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.			MH
MP-4	<b>Media Storage:</b> The organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.			MH
MP-5	<b>Media Transport:</b> The organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.			MH
MP-6	<b>Media Sanitization:</b> The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.			MH
MP-7	<b>Media Destruction and Disposal:</b> The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized			A

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	individuals from gaining access to and using the information contained on the media.			

## B12 Incident Response (IR)

The status of incident response controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
<b>IR-1</b>	<b>Incident Response Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.			<b>A</b>
<b>IR-2</b>	<b>Incident Response Training:</b> The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.			<b>MH</b>
<b>IR-2 (1)</b>	<b>Incident Response Training:</b> The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.			<b>MH</b>
<b>IR-2 (2)</b>	<b>Incident Response Training:</b> The organization employs automated mechanisms to provide a more thorough and realistic training environment.			<b>H</b>
<b>IR-3</b>	<b>Incident Response Testing:</b> The organization tests the incident response capability for the information system at least annually using automated mechanisms for high systems to determine the incident response effectiveness and documents the results.			<b>MH</b>
<b>IR-3 (1)</b>	<b>Incident Response Testing:</b> The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.			<b>H</b>
<b>IR-4</b>	<b>Incident Handling:</b> The organization implements an incident			<b>A</b>

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.			
<b>IR-4 (1)</b>	<b>Incident Handling:</b> The organization employs automated mechanisms to support the incident handling process.			<b>MH</b>
<b>IR-5</b>	<b>Incident Monitoring:</b> The organization tracks and documents information system security incidents on an ongoing basis.			<b>MH</b>
<b>IR-5 (1)</b>	<b>Incident Monitoring:</b> The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.			<b>H</b>
<b>IR-6</b>	<b>Incident Reporting:</b> The organization promptly reports incident information to appropriate authorities.			<b>A</b>
<b>IR-6 (1)</b>	<b>Incident Reporting:</b> The organization employs automated mechanisms to assist in the reporting of security incidents.			<b>MH</b>
<b>IR-7</b>	<b>Incident Response Assistance:</b> The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization’s incident response capability.			<b>A</b>
<b>IR-7 (1)</b>	<b>Incident Response Assistance:</b> The organization employs automated mechanisms to increase the availability of incident response-related information and support.			<b>MH</b>

## B13 Awareness and Training (AT)

The status of awareness and training controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
<b>AT-1</b>	<b>Security Awareness and Training Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles,			<b>A</b>

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.			
AT-2	<b>Security Awareness:</b> The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.			A
AT-3	<b>Security Training:</b> The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and each year thereafter.			A
AT-4	<b>Security Training Records:</b> The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.			A

## B14-B17 TECHNICAL CONTROLS

This section describes the level of implementation of technical controls for the [System Name].

### B14 Identification and Authentication (IA)

The status of identification and authentication controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
IA-1	<b>Identification and Authentication Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.			A

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
IA-2	<b>User Identification and Authentication:</b> The information system uniquely identifies and authenticates users (or processes acting on behalf of users).			A
IA-2 (1)	<b>User Identification and Authentication:</b> The information system employs multifactor authentication.			H
IA-3E	<b>Device Identification and Authentication:</b> The information system identifies and authenticates specific devices before establishing a connection.			MH
IA-4	<b>Identifier Management:</b> The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after 30 days of inactivity; and (vi) archiving user identifiers.			A
IA-5	<b>Authenticator Management:</b> The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.			A
IA-6	<b>Authenticator Feedback:</b> The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.			A
IA-7	<b>Cryptographic Module Authentication:</b> For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.			A

## B15 Access Control (AC)

The status of access controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

OFFICIAL USE ONLY

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
AC-1	<b>Access Control Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.			A
AC-2	<b>Account Management:</b> The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts annually.			A
AC-2 (1)	<b>Account Management:</b> The organization employs automated mechanisms to support the management of information system accounts.			MH
AC-2 (2)	<b>Account Management:</b> The information system automatically terminates temporary and emergency accounts after 48 hours.			MH
AC-2 (3)	<b>Account Management:</b> The information system automatically disables inactive accounts after 90 days.			MH
AC-2 (4)	<b>Account Management:</b> The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.			H
AC-3	<b>Access Enforcement:</b> The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.			A
AC-3 (1)	<b>Access Enforcement:</b> The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).			MH
AC-4	<b>Information Flow Enforcement:</b> The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.			MH
AC-5	<b>Separation of Duties:</b> The information system enforces separation of duties through assigned access authorizations.			MH
AC-6	<b>Least Privilege:</b> The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of			MH

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	specified tasks.			
AC-7	<b>Unsuccessful Logon Attempts:</b> The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account/node for 30 minutes for low systems or until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.			A
AC-7 (1)	<b>Unsuccessful Logon Attempts:</b> The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.			RB
AC-8	<b>System Use Notification:</b> The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.			A
AC-9	<b>Previous Logon Notification:</b> The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.			RB
AC-10	<b>Concurrent Session Control:</b> The information system does not allow concurrent sessions.			H
AC-11	<b>Session Lock:</b> The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.			MH
AC-12	<b>Session Termination:</b> The information system automatically terminates a session after ten minutes of inactivity.			MH
AC-13	<b>Supervision and Review—Access Control:</b> The organization supervises and reviews the activities of users with respect to the			A

OFFICIAL USE ONLY

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	enforcement and usage of information system access controls.			
AC-13 (1)	<b>Supervision and Review—Access Control:</b> The organization employs automated mechanisms to facilitate the review of user activities.			H
AC-14	<b>Permitted Actions w/o Identification or Authentication:</b> The organization identifies specific user actions that can be performed on the information system without identification or authentication.			A
AC-14 (1)	<b>Permitted Actions w/o Identification or Authentication:</b> The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.			MH
AC-15	<b>Automated Marking:</b> The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.			H
AC-16	<b>Automated Labeling:</b> The information system appropriately labels information in storage, in process, and in transmission.			RB
AC-17	<b>Remote Access:</b> The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.			A
AC-17 (1)	<b>Remote Access:</b> The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.			MH
AC-17 (2)	<b>Remote Access:</b> The organization uses encryption to protect the confidentiality of remote access sessions.			MH
AC-17 (3)	<b>Remote Access:</b> The organization controls all remote accesses through a managed access control point.			MH
AC-18	<b>Wireless Access Restrictions:</b> The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.			MH
AC-18 (1)	<b>Wireless Access Restrictions:</b> The organization uses authentication and encryption to protect wireless access to the			MH

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	information system.			
AC-19	<b>Access Control for Portable and Mobile Systems:</b> The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.			MH
AC-19 (1)	<b>Access Control for Portable and Mobile Systems:</b> The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.			H
AC-20	<b>Personally Owned Information Systems:</b> The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.			A

## B16 Audit and Accountability (AU)

The status of audit and accountability controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
AU-1	<b>Audit and Accountability Policy and Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.			A
AU-2	<b>Auditable Events:</b> The information system generates audit records for events identified in the HUD IT Security Handbook.			A
AU-2 (1)	<b>Auditable Events:</b> The information system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical),			RB

OFFICIAL USE ONLY

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
	time-correlated audit trail.			
AU-2 (2)	<b>Auditable Events:</b> The information system provides the capability to manage the selection of events to be audited by individual components of the system.			RB
AU-3	<b>Content of Audit Records:</b> The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.			A
AU-3 (1)	<b>Content of Audit Records:</b> The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.			MH
AU-3 (2)	<b>Content of Audit Records:</b> The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.			H
AU-4	<b>Audit Storage Capacity:</b> The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.			A
AU-5	<b>Audit Processing:</b> In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: <ul style="list-style-type: none"> <li>• Shutdown the system</li> <li>• Overwrite the oldest audit records</li> <li>• Stop generating audit records</li> </ul>			A
AU-5 (1)	<b>Audit Processing:</b> The information system provides a warning when allocated audit record storage volume is close to being reached.			H
AU-6	<b>Audit Monitoring, Analysis, and Reporting:</b> The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.			MH
AU-6 (1)	<b>Audit Monitoring, Analysis, and Reporting:</b> The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.			H

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
AU-6 (2)	<b>Audit Monitoring, Analysis, and Reporting:</b> The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.			RB
AU-7	<b>Audit Reduction and Report Generation:</b> The information system provides an audit reduction and report generation capability.			MH
AU-7 (1)	<b>Place Holder:</b> The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.			H
AU-8	<b>Time Stamps:</b> The information system provides time stamps for use in audit record generation.			MH
AU-9	<b>Protection of Audit Information:</b> The information system protects audit information and audit tools from unauthorized access, modification, and deletion.			A
AU-9 (1)	<b>Protection of Audit Information:</b> The information system produces audit information on hardware-enforced, write-once media.			RB
AU-10	<b>Non-repudiation:</b> The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).			RB
AU-11	<b>Audit Retention:</b> The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.			A

## B17 System and Communications Protection (SC)

The status of system and communications protection controls for the [System Name] is as indicated in the following table:

[Use the Not Applicable column to identify the controls applicable to the system. A=all systems; MH=Moderate and High systems; H=high systems only. Mark those that are not applicable as “NA”; do not delete them.]

Control Number	Description of Control [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	In Place	Planned	Not Applicable
SC-1	<b>System &amp; Communications Protection Policy &amp; Procedures:</b> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.			A
SC-2	<b>Application Partitioning:</b> The information system separates user functionality (including user interface services) from information system management functionality.			MH
SC-3	<b>Security Function Isolation:</b> The information system isolates security functions from non-security functions.			H
SC-3 (1)	<b>Security Function Isolation:</b> The information system employs underlying hardware separation mechanisms to facilitate security function isolation.			H
SC-3 (2)	<b>Security Function Isolation:</b> The information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both non-security functions and from other security functions.			H
SC-3 (3)	<b>Security Function Isolation:</b> The information system minimizes the amount of non-security functions included within the isolation boundary containing security functions.			H
SC-3 (4)	<b>Security Function Isolation:</b> The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.			H
SC-3 (5)	<b>Security Function Isolation:</b> The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.			H
SC-4	<b>Information Remnants:</b> The information system prevents unauthorized and unintended information transfer via shared system resources.			MH
SC-5	<b>Denial of Service Protection:</b> The information system protects against or limits the effects of denial of service attacks on devices within the organization's internal network.			A
SC-5 (1)	<b>Denial of Service Protection:</b> The information system restricts			RB

OFFICIAL USE ONLY

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
	the ability of users to launch denial of service attacks against other information systems or networks.			
<b>SC-5 (2)</b>	<b>Denial of Service Protection:</b> The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.			<b>RB</b>
<b>SC-6</b>	<b>Resource Priority:</b> The information system limits the use of resources by priority.			<b>MH</b>
<b>SC-7</b>	<b>Boundary Protection:</b> The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.			<b>A</b>
<b>SC-7 (1)</b>	<b>Boundary Protection:</b> The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.			<b>MH</b>
<b>SC-8</b>	<b>Transmission Integrity:</b> The information system protects the integrity of transmitted information.			<b>MH</b>
<b>SC-8 (1)</b>	<b>Transmission Integrity:</b> The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).			<b>H</b>
<b>SC-9</b>	<b>Transmission Confidentiality:</b> The information system protects the confidentiality of transmitted information.			<b>MH</b>
<b>SC-9 (1)</b>	<b>Transmission Confidentiality:</b> The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).			<b>H</b>
<b>SC-10</b>	<b>Network Disconnect:</b> The information system terminates a network connection at the end of a session or after ten minutes of inactivity.			<b>MH</b>
<b>SC-11</b>	<b>Trusted Path:</b> The information system establishes a trusted communications path between the user and the security functionality of the system.			<b>RB</b>

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
SC-12	<b>Cryptographic Key Establishment and Management:</b> The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.			MH
SC-13	<b>Use of Validated Cryptography:</b> When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.			A
SC-14	<b>Public Access Protections:</b> For publicly available systems, the information system protects the integrity of the information and applications.			A
SC-15	<b>Collaborative Computing:</b> The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).			MH
SC-15 (1)	<b>Collaborative Computing:</b> The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.			RB
SC-16	<b>Transmission of Security Parameters:</b> The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.			RB
SC-17	<b>Public Key Infrastructure Certificates:</b> The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.			MH
SC-18	<b>Mobile Code:</b> The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.			MH
SC-19	<b>Voice Over Internet Protocol:</b> The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize			MH

OFFICIAL USE ONLY

<b>Control Number</b>	<b>Description of Control</b> [Document how the control has been specifically implemented for the system; describe actions that are planned to complete implementation]	<b>In Place</b>	<b>Planned</b>	<b>Not Applicable</b>
	the use of VOIP.			

## Appendix A – [SYSTEM NAME] Rules of Behavior

Below is a template for writing Rules of Behavior (ROB) for your organization. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 recommends that the ROB be included in the System Security Plan (SSP) as an appendix such as this.

### 1. Responsibilities

**Discussion:** In this section, you will need to describe what ROB are, why they are needed, what users can expect, and the consequences for violating ROB. Sample language for completing this section is provided below.

#### Sample Language:

*What are Rules of Behavior?*

Office of Management and Budget (OMB) Circular A-130 Appendix III requires every System Security Plan (SSP) to contain a Rules of Behavior (ROB). ROB apply to the system users and list specific responsibilities and expected behavior of all individuals with access to or use of the named information system. In addition, ROB outlines the consequences of non-compliance and/or violations.

*Why are Rules of Behavior Needed?*

ROB is part of a complete program to provide good information security and raise security awareness. ROB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

*Who is Covered by the Rules of Behavior?*

The ROB covers all government and non-government users of the named information systems. This includes contract personnel and other federally funded users.

*What are the Consequences for Violating the Rules of Behavior?*

Penalties for non-compliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

### 2. Application and Organization Rules

**Discussion:** In this section you will list the ROB measures that will apply to application users and the organization in general. Section 3.1 lists the most common and minimal set of ROB as recommended by NIST 800-18. Section 3.2 lists other ROB that may apply to your organization. Section 2h includes ROB for system administrators. Each section is discussed in detail below.

**Note:** The sample ROB that appear below are very restrictive. It is understood that certain organizations allow flexibility (i.e. computers may be used on a limited basis for personal use) and therefore ROB should be adjusted accordingly. In addition, not all samples listed below will apply to your system or organization. You may find it necessary to modify some samples to comply with your specific needs and requirements.

**Discussion:** The following categories are the most common ROB. These categories are listed in NIST 800-18 as the “minimal” recommended set of ROB that an organization should have. Sample language for each category is provided below.

Sample Language:

*A. Passwords*

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as \*#\$ %). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other’s password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.
5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

*B. Encryption*

1. Extremely sensitive data should be encrypted prior to transmission.
2. The sensitivity of the information needing protection, among other considerations, determines the sophistication of the encryption technology. In most circumstances, only the most sensitive or compartmentalized information should be encrypted.
3. Files that contain passwords, proprietary, personnel, or business information, and financial data typically require encryption before transmission, and should be encrypted while stored on the computer’s hard disk drive.
4. Sensitive information that travels over wireless networks and devices should be encrypted.

*C. Internet Usage*

1. Downloading files, programs, templates, images, and messages, except those explicitly authorized and approved by the system administrator, is prohibited.
2. Visiting websites including, but not limited to, those that promote, display, discuss, share, or distribute hateful, racist, pornographic, explicit, or illegal activity is strictly prohibited.
3. Because they pose a potential security risk, the use of Web based instant messaging or communication software or devices are prohibited.
4. Using the Internet to make non-work related purchases or acquisitions is prohibited.
5. Using the Internet to manage, run, supervise, or conduct personal business enterprises is prohibited.

*D. Email*

1. Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited.
2. E-mail addresses and e-mail list-serves constitute sensitive information and are never to be sold, shared, disseminated, or used in any unofficial manner.
3. Using an official e-mail address to subscribe to any non-work related electronically distributed newsletter or magazine is prohibited.

*E. Working from Home/Remote Dial-up Access*

1. Users may dial into the network remotely only if pre-approved by the system administrator.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. At no time should a "live" dial-up connection be left unattended.
4. Web browsers must be configured to limit vulnerability to an intrusion and increase security.
5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install a hardware or software firewall.
6. No official material may be stored on the user's personal computer. All data must be stored on a floppy disk and then secured in a locked filing cabinet, locker, etc.
7. Operating system configurations should be selected to increase security.

*F. Unofficial Use of Government Equipment*

Except for limited personal use, government equipment including, but not limited to, fax machines, copying machines, postage machines, telephones, and computers are for official use only.

*G. Other Rules of Behavior*

**Discussion:** Section 3 lists the most common ROB categories as recommended by NIST 800-18. However, there are other ROB, which may apply to your organization. You will want to include these rules here, in Section 3. Note: It is not necessary to begin a new section or to differentiate between the types of rules (i.e. "most common" vs. "other").

These additional ROB that may apply appear below.

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.
2. Users who no longer require IT system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the system administrator.
3. When not in use, workstations must be physically secured. Users must also log-off or turn-off the system.
4. Screen-savers must be password protected.

5. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
6. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
7. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.

#### *H. Additional Rules of Behavior for System Administrators*

**Note:** This section only applies to system administrators. If you are writing a ROB for system users, you may skip this section and continue to Section 3.

**Discussion:** system administrators have a unique responsibility above and beyond that of regular users. In addition to being regular system users, they also have special access privileges that regular users do not have. Therefore, they need to be susceptible to additional ROB over and above the common user.

**System User vs. System Administrator Option:** You may find it easier to create two separate ROB documents – one for system users and the other for system administrators. The system users ROB would include sections 3.1 and 3.2 only, while the “system administrators” ROB would include sections 3.1-3.3. Alternatively, you could create one ROB document noting that this section would only apply to system administrators.

#### Sample Rules of Behavior Language for System Administrators:

1. System administrators may only access or view user accounts with the expressed consent of the user and/or management.
2. System administrators may not track or audit user accounts without the expressed consent of the user and/or management.
3. System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. It is the system administrators' responsibility to account for all system hardware and software loaned to system users for the execution of their official duties.

### **3. Acknowledgment**

**Discussion:** In this section, you will create a signature page. Prior to receiving authorization for system access, every user should read and sign the ROB (this includes system administrators since they are also “users” of the system). By signing the signature page, the user agrees to abide by the ROB and understands that failure to do so might be grounds for disciplinary action.

Ensure that users retain a copy of their signed ROB for their records.

**I have read and understand the Rules of Behavior governing my use of **System Name** and agree to abide by them. I understand that failure to do so may result in disciplinary action being brought against me.**

OFFICIAL USE ONLY

User Name (please print) \_\_\_\_\_

User Signature \_\_\_\_\_

Organization \_\_\_\_\_

Date \_\_\_\_\_

## INDEX

Applicable Laws or Regulations Affecting the System .....	6	NIST Special Publication (SP) 800-26, Security Self-Assessment Guide for Information Technology .....	vi
<b>Audit Trails</b> .....	43	Office of Management and Budget (OMB) Circular A-130 .....	vi, 4, 1
Authorize Processing (C&A) .....	19	Operational Controls .....	20
<b>Availability</b> .....	6, 7, 8, 10, 13	Operational Status .....	2
Computer Security Act of 1987 .....	vi	<i>Password</i> .....	2, 3
<b>Confidentiality</b> .....	6, 7, 8, 10, 12	<b>Personnel Security</b> .....	20
Contact(s) .....	1	Physical and Environmental Protection .....	22
Data Integrity .....	32	Rules of Behavior .....	5, 1, 3, 4
Description/Purpose .....	3	Security Controls .....	vi, 5, 9, 12
Documentation .....	vi	Security Responsibility .....	2
<b>Encryption</b> .....	2	Sensitivity .....	4, 6, 7, 12
Identification and Authentication .....	38	System Environment .....	3
Information Categories .....	7	System Identification .....	1, 14
<b>Integrity</b> .....	6, 7, 8, 10, 13	System Interconnection/Information Sharing ...	4
Logical Access Controls .....	40	System Security Plan .....	vi
Management Controls .....	15	Technical Controls .....	38
Management of Federal Information Resources and Public Law 100-235 .....	vi		
NIST Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems .....	vi		