[Insert System Name (Acronym)]

Security Categorization: Moderate

System System Security Plan

Version *[Insert #]*

[Insert Date]

Prepared by

[Insert Group/Organization/Company Name]
[Insert Street Address]
[Insert City, State, and Zip Code]

[This sample format provides a template for preparing a System Security Plan for System certification and accreditation (C&A) processing. The template is intended to be used as a guide, and the preparer should modify the format as necessary to meet the system's security controls and comply with internal policies. Where practical, the guide provides instructions [in blue, bolded text] for completing specific sections.

Remove this page before releasing the first draft.

DOCUMENT CHANGE CONTROL

Version	Release Date	Summary of Changes	Addendum Number[1]	Name
[Version 0.1]	*[Insert Date]*	*[First Draft – Initial draft.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 0.2]	*[Insert Date]*	*[Second Draft – Incorporates information collected from working session with stakeholders.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 0.3]	*[Insert Date]*	*[Third Draft – Incorporates changes from C&A Team QC.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 0.4]	*[Insert Date]*	*[Fourth Draft – Incorporates changes from validation session with stakeholders.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 0.5]	*[Insert Date]*	*[Fifth Draft – Incorporates changes from collaboration meeting on the ST&E plan with stakeholders.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 0.6]	*[Insert Date]*	*[Sixth Draft – Incorporates changes based on ST&E findings.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 0.9]	*[Insert Date]*	*[Ninth Draft – Final Draft.]*	*[Insert Addendum #]*	*[Insert Name]*
[Version 1.0]	*[Insert Date]*	*[First Release.]*	*[Insert Addendum #]*	*[Insert Name]*

[1] *Minor changes should be recorded in the addendum section of this document. These changes must be incorporated into the main document upon the next full document release (at least annually).*

TABLE OF CONTENTS

1. PREFACE

[Insert System Name (Acronym)] is an ***[Insert Group/Organization/Company]*** application/system that has been categorized as a ***[Insert 'Major' or 'Minor']*** System. ***[Insert System Acronym] [Insert 'will reside' or 'currently resides']*** on a ***[Insert system operating system(s)]*** platform and ***[Insert 'is targeted for deployment by' or 'has been deployed since'] [Insert Deployment Date]***. ***[Insert General Description of the System]***.

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

- *Federal Information Security Management Act (FISMA) of 2002, Title III – Information Security*, P.L. 107-347: A security plan must be developed and practiced throughout all life cycles of the agency's information systems.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*: A System Security Plan (SSP) is to be developed and documented for each GSS and Major System (MA) consistent with guidance issued by the National Institute of Standards and Technology (NIST).
- Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*: This document defines standards for the security categorization information and information systems. System security categorization must be included in SSPs.
- Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*: This document contains information regarding specifications for minimum security control requirements for Federal information and information systems. Minimum security controls must be documented in SSPs.
- NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems*: The minimum standards for an SSP are provided in this NIST document.
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems:* This document contains a list of security controls that are to be implemented into Federal information systems based on their FIPS 199 categorization. This document is used in conjunction with FIPS 200 to define minimum security controls, which must be documented in SSPs.

The SSP documents the current and planned controls for the system and addresses security concerns that may affect the system's operating environment. Security categorization of federal information systems, as required by FIPS 199, is the first step in selecting appropriate system security controls. FIPS 199 categories are derived according to the potential impact on a system that would occur if its Confidentiality, Integrity, or Availability were compromised. FIPS 199 category definitions are as follows:

- *High Impact:* The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- *Moderate Impact:* The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- *Low Impact:* The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Subsequent to the security categorization process, an appropriate set of security controls must be selected, which satisfy the minimum security requirements set forth in FIPS 200. The selected set of security controls must be one of three security control baselines (high, moderate, low) from NIST SP 800-53 that are associated with the designated impact levels of the agency information systems as determined during the security categorization process. Each of the selected controls is documented in Minimum Security Controls section of this SSP and has been given one of the implementation statuses that are described below:

- **In Place** – The control is fully in place as described in NIST SP 800-53.
- **Partially In Place** – Aspects of the NIST SP 800-53 control are in place, but part of the control is either planned to be satisfied or a risk based decision has been put in place not to fully satisfy the control per NIST SP 800-53.
- **Planned** – The control is not in place and there is a planned activity to implement the control.
- **Risk Based Decision** – The control is not in place and there has been a decision reached not to put the control in place based on risk factors.
- **Inherited** – The control is either implemented at the organization level or is implemented by a GSS.
- **Not Applicable** – The control does not apply to the system under consideration. If this status is selected for a control, an explanation should be provided in the 'Implementation of Control' field.

This SSP will be part of the certification and accreditation (C&A) package submitted to and approved by the Certifier and the Designated Approving Authority (DAA), who will authorize the system to operate.

The format of this SSP was developed in accordance with the *Guide for Developing Security Plans for Information Technology Systems* (NIST SP 800-18). The DAA must authorize all changes to the system SSP. The information system owner will be responsible for assigning an authoritative source to make these changes and ensure that multiple persons do not change the document simultaneously. Plan modifications and changes must be logged in the document configuration control table (see page i). Version numbers will reflect the magnitude of change to the document. Significant changes will be denoted by a version increase of a whole number, such as from 1.0 to 2.0. Minor changes will be denoted by a version increase of a fractional increment, such as from 1.0 to 1.1. A detailed description of minor plan modifications and changes not yet incorporated in a new version will be included in the Addendum section of this document.

2. SYSTEM IDENTIFICATION

2.1 System Name/Title/Unique Identifier

System Name: ***[Insert System Name (Acronym)]***
Unique Identifier: ***[Insert Unique Identifier. The Unique Identifier may be the System's Unique Project Identifier (UPI) from the OMB Exhibit 300 or Exhibit 53 or an Organization Defined Identifier. Remove the Unique Identifier line if one does not exist.]***

2.2 Security Categorization

This system has been categorized as Moderate risk according to FIPS 199. Refer to Appendix E for supporting documentation regarding the determination of the system's security categorization.

2.2.1 Information System Type

The ***[Insert System Acronym]*** application is a ***[Insert 'Major' or 'Minor']*** system.

2.2.2 Security Control Selection

The system must meet the FIPS 200 minimum security requirements by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53. The process of selecting the appropriate security controls and assurance requirements for agency information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the agency. Security categorization of federal information and information systems, as required by FIPS 199, is the first step in the risk management process. Subsequent to the security categorization process, an agency must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in FIPS 200. The selected set of security controls must be one of three security control baselines (high, moderate, low) from NIST SP 800-53 that are associated with the designated impact levels of the agency information systems as determined during the security categorization process.

2.2.3 Common Controls

Some controls within this plan are referred to as common controls. Common controls, as defined by NIST 800-53 are controls in which the implementation is managed by an organizational entity other than the system owner. Within the organization environment, there are three types of common controls:

- **Organizational Common Controls** – controls implemented centrally at enterprise-wide level that are implemented commonly for all the systems e.g. policies and procedures. Unless there is uniqueness, these controls are outside the direct control of the system owner, and are centrally maintained and managed. The implementation of these controls is documented in the SSP. However, these controls are verified once through ST&E and the results are reused in each system C&A package.

- **GSS Common Controls** – controls that rely on a GSS for implementation (e.g., Incident Response controls). Since the implementation of common controls is the responsibility of another organizational entity, these controls are documented and assessed as part of that entity's C&A efforts, and therefore is not assessed as part of this system C&A.

[Some of the common controls can turn out to be hybrid controls, which means the control may contain elements of a common control, and elements of an system-specific control. Use the common control language as a starting point for discussion of these control with the system owner. Recommend to share the SSP with the POCs to let then review and make changes to these controls. Allocate some time in the working session agenda to discuss those changes made by the POCs and then document using the guidance below:

If the system does not have any processes or procedures above what is in the common control language, then that language will suffice. No further action needed.

If the system has specific processes and procedures above what is in the common control language, document those in addition to the common control language, flag them with "Unique Implementation:", and place that write-up towards the end of the paragraph addressing the implementation of the control.

If the system hardware is housed at non-organization facilities (e.g. contractor or other government agency), common controls may not be applicable and these controls will need to be fully documented and tested.

2.3 Information System Security Plan Completion Date

Refer to the cover page of this document for the SSP Completion Date.

2.4 Information System Security Plan Approval Date

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

2.5 System Owner

Name:	[*Insert Name of System Owner*]
Office Symbol:	[*Insert Office Symbol*]
Title:	[*Insert Job Title*]
Agency:	*[Insert Group/Organization/Company]*
Address:	[*Insert Street Address*] [*Insert Building and Room Number*] [*Insert City, State, and Zip*]
Telephone:	[*Insert Telephone Number*]
Email:	[*Insert Email Address*]

Responsibility:	The System Owner is responsible for defining the system's operating parameters, authorized functions, and security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. In addition, a single system may utilize information from multiple Information Owners. ***Note: The system owner and the authorizing official may be the same individual.***

2.6 Authorizing Official

Name:	[***Insert Name of Authorizing Official***]
Office Symbol:	[***Insert Office Symbol***]
Title:	[***Insert Job Title***]
Agency:	***[Insert Group/Organization/Company]***
Address:	[***Insert Street Address***] [***Insert Building and Room Number***] [***Insert City, State, and Zip***]
Telephone:	[***Insert Telephone Number***]
Email:	[***Insert Email Address***]
Responsibility:	Senior management official who has the authority to authorize processing (accredit) ***and*** accept the risk associated with the system. ***Note: The system owner and the authorizing official may be the same individual.***

2.7 Other Designated Contacts

[Include other individuals who have significant responsibilities regarding the system and can provide valuable insight concerning the information contained in this SSP. Examples include: system administrator, security administrator, database administrator, and relevant site personnel. Provide a custom description for each individual's responsibilities. Create additional tables for as many individuals in this section as necessary.]

Name:	[***Insert Name of Other Designated Contact***]
Office Symbol:	[***Insert Office Symbol***]
Title:	[***Insert Job Title***]
Agency:	***[Insert Group/Organization/Company]***
Address:	[***Insert Street Address***] [***Insert Building and Room Number***] [***Insert City, State, and Zip***]
Telephone:	[***Insert Telephone Number***]
Email:	[***Insert Email Address***]
Responsibility:	***[Include custom description of the individual's responsibilities.]***

2.8 Assignment of Security Responsibility

Name:	[***Insert Name of Other Designated Contact***]
Office Symbol:	[***Insert Office Symbol***]
Title:	[***Insert Job Title***]
Agency:	***[Insert Group/Organization/Company]***

Address:	[***Insert Street Address***] [***Insert Building and Room Number***] [***Insert City, State, and Zip***]
Telephone:	[***Insert Telephone Number***]
Email:	[***Insert Email Address***]
Responsibility:	Assigned responsibility, in writing, to ensure that the system has adequate security measures built into the system. This individual will be knowledgeable of the management, operational, and technical controls used to protect the system as well as specific FISMA and C&A information.

2.9 System Operational Status

[Insert System Acronym] is currently in the ***[Insert Phase]*** phase in accordance with the system development life cycle (SDLC) as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18. ***[Insert System Acronym] [Insert 'is targeted for deployment by' or 'has been deployed since'] [Insert Deployment Date]***.

[Indicate status of the system:

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

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

2.10 Privacy Considerations

Section 208 of the E-Government Act of 2002 and Section 522 of the Consolidated Appropriations Act of 2005 require that when developing or procuring IT systems or projects that collect, use, store, and/or disclose information in identifiable form from or about members of the public or agency employees [the latter prescribed by Sect. 522], to identify potential privacy risks and implement appropriate privacy controls and compliance requirements. ***[Insert System Acronym] [Insert 'does' or 'does not']*** contain privacy information. ***[If the system contains privacy data, insert a reference to privacy related documentation (e.g., A Privacy Impact Assessment (PIA) was conducted as part of the current C&A process. Refer to the [Insert System Acronym] PIA Questionnaire in Appendix I of this SSP for further information. A signed PIA memo is provided in Appendix D of the [Insert System Acronym] Security Assessment Report (SAR)].***

2.11 Disclosure Considerations

The Privacy Act requires agencies to publish Systems of Records Notices (SORNs) that describe the categories of personally identifiable information that they collect, maintain and use. ***[Insert***

System Acronym] [Insert whether the system does or does not require a SORN] require a System of Records Notice (SORN). ***[If the system requires a SORN, insert a reference to related documentation (e.g. The following SORN(s) is/are identified for [Insert System Acronym].]***

- ***[Insert applicable SORN(s) for each bullet item.]***

2.12 e-Authentication

According to OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, e-Authentication is defined as the process of establishing confidence in user identities electronically presented to an information system. OMB M-04-04 states that e-Authentication "applies to all [Federal Electronic] transactions for which authentication *is* required, regardless of the constituency (e.g. individual user, business, or government entity)." OMB guidance provides assistance to federal agencies in determining the appropriate level of assurance for electronic transactions requiring authentication by establishing and describing four levels of identity assurance, as well as providing strategies for determining which of these levels is appropriate for the information system.

In accordance with OMB M-04-04, all federal agencies must conduct an e-Authentication risk assessment on those systems that remotely authenticate users over a network for purposes of e-government and commerce in order to determine the required level of authentication assurance for the information system. Once an e-Authentication risk assessment has been preformed and an overall assurance level has been determined, OMB M-04-04 recommends that agencies use NIST Special Publication (SP) 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, to "select the appropriate [authentication] technology that, at a minimum, meets the technical requirements for the required level of assurance."

In addition, Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, recommends that owners of logical resources apply OMB Memorandum M-04-04 Guidance to identify the level of assurance required for their electronic transaction.

Use the following for systems requiring e-Authentication:
[Insert System Acronym] has been identified as an system that requires an e-Authentication risk assessment in accordance with OMB Memo 04-04. ***[Insert System Acronym]*** is operating under Assurance Level ***[Insert Assurance Level]***. Refer to Appendix H for further information on e-Authentication.

Or

Use the following for systems NOT requiring e-Authentication:
[Insert System Acronym] has been determined to be a Federal System that does not require e-Authentication security controls to be implemented due to the nature of the transactions processed on the system.

2.13 General Description/Purpose

[Insert a description of the function and purpose of the system (e.g., tax administration, network support, data analysis). Provide a description of the applets, subsystems, modules that comprise the system (this can either go in this section of the System Environment section). 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.]

2.14 System Environment

[Insert detailed description of the technical environment of the System, including information such as the name and description of system software and how the System is accessed by users (e.g., via Intranet). In addition, discuss the GSS on which the System resides and include a reference to the GSS SSP. Include any environmental or technical factors that raise special security concerns.

In addition, provide a System/Network Diagram in Appendix C and an Input/Output Diagram in Appendix D of this SSP.]

Hardware Component	Operating System and Version	Database(s) and Version(s)	Software and Version(s)	Supported Modules	Location(s)

2.15 System Interconnection/Information Sharing

[Insert description of existing system interconnections/interfaces and connections with other systems. This includes information shared via tape, FTP, etc. Any system that sends data to or receives data from the system should be listed here. In addition describe how shared information is protected if the system/system is interconnected with systems/systems external to the organization. For system/systems that are interconnected with systems external to the organization, include information regarding specific information within one combined "Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) document. Attach copies of the MOU/ISA memos in Appendix F of this SSP and reference this appendix.

System Name	Organization	Type (TCP/IP, Dial-up, SNA, etc.)	Authorizations (MOU/ISA)	Date of Agreement	FIPS 199 Category	C&A Status of the System	Name and Title of Authorizing Official

2.16 Laws, Regulations, and Policies Affecting the System

The laws, Executive Orders, regulations, and policies that establish specific requirements for the confidentiality, integrity, or availability of the data processed, stored, and transmitted by the system are provided in the Preface and Appendix B (comprehensive listing).

3. MANAGEMENT CONTROLS

This section describes the management control measures intended to meet the systems security requirements. Management controls focus on the management of risk in operating the system.

3.1 Risk Assessment (RA) Controls

The following section will discuss the risk assessment family of controls that are used to identify threats to and vulnerabilities of a system. Analysis is used as a basis for identifying and selecting appropriate and cost-effective measures.

3.1.1 RA-1: Risk Assessment Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.1.2 RA-2: Security Categorization

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The applicable federal standard for security categorization of nonnational security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. Related security controls: MP-4, SC-7.
NIST SP 800-53A Control Expected Results: (1) System's System Security Plan contains the security categorization, including supporting rationale. (2) Security categorization was performed in accordance with FIPS PUB 199. (3) Security categorization has been approved by the designated senior-level

official and name of the official and approval date are recorded. (4) The security categorization process is conducted as an organization-wide exercise that include authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners.
Personally Identifiable Information Mapping: OMB M-06-16, Action Item 1.1 **Personally Identifiable Information Guidance:** Ensure the security categorization explicitly identifies PII data remotely accessible or physically removed.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.1.3 RA-3: Risk Assessment

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 (including information and information systems managed/operated by external parties).
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.
NIST SP 800-53A Control Expected Results: (1) Risk assessments are conducted and documented and include magnitude of harm that could result from the unauthorized access, use, disclosure, modification, or destruction of the information and the information systems that support its operations and assets (including information and information systems managed/operated by external parties). (2) The risk assessment for the information system to determine if the assessment is consistent with NIST Special Publications 800-30 and 800- 95.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.1.4 RA-4: Risk Assessment Update

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization updates the risk assessment [*Assignment: organization-*

defined frequency] 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.
NIST SP 800-53A Control Expected Results: (1) The Risk Assessment is updated in accordance with organization-defined frequency 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. (2) The risk assessment was performed within the organization-defined frequency or since there was a major change to the system, the facilities where the system resides, or other conditions that may have had an impact to the security or accreditation status of the system.
Personally Identifiable Information Mapping: OMB M-06-16, Action Item 1.2 **Personally Identifiable Information Guidance:** Ensure the risk assessment accurately depicts the risks associated with remote access and physical removal of PII data.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.1.5 RA-5: Vulnerability Scanning

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities affecting the system are identified and reported.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and systems may require additional, more specialized approaches (e.g., vulnerability scanning tools for systems, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.2 Planning (PL) Controls

The following management control family section will address the security planning that occurs for the system.

3.2.1 PL-1: Security Planning Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.2.2 PL-2: System Security Plan

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture. NIST Special Publication 800-18 provides guidance on security planning.
NIST SP 800-53A Control Expected Results: (1) The system security plan document for the system exists and title and date/version of the document is recorded. (2) The system security plan is disseminated to appropriate elements within the organization. (3) The system security plan was reviewed and approved by designated officials and name of individual(s) is recorded. (4) The system security plan was developed in accordance with NIST SP 800-18. (5) Key operating elements within the organization understand the security plan and are ready to implement the plan.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.2.3 PL-3: System Security Plan Update

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.
NIST SP 800-53A Control Expected Results: (1) The system security plan is reviewed by

organization-defined frequency. During reviews, major changes to the organization and/or system, problems with security plan implementation, and security control enhancements are considered for updates. (2) The revised plan reflects the needed changes based on the organization's experiences.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.2.4 PL-4: Rules of Behavior

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 and its resident information.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.2.5 PL-5: Privacy Impact Assessment

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization conducts a privacy impact assessment on the information system.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.
NIST SP 800-53A Control Expected Results: (1) The privacy impact assessment adequately addresses the areas identified in the organizational privacy impact assessment policy.
Personally Identifiable Information Mapping: OMB M-06-16, Action Item 1.1 **Personally Identifiable Information Guidance:** Ensure the PIA identifies PII data, how it is protected when access remotely or physically removed, and states the potential impact on privacy if the data were lost, corrupted, accessed by an unauthorized individual, etc.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.2.6 PL-6: Security-Related Activity Planning

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization ensures that appropriate planning and coordination occur before conducting security-related activities affecting the information system in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.

NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.
NIST SP 800-53A Control Expected Results: (1) All security-related activities that effect the system are planned and coordinated. (2) All key operating elements within the organization understand the breath and depth of ongoing security-related activities in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3 System and Services Acquisition (SA) Controls

The following sections will discuss system controls pertaining to the acquisition of hardware, software, and firmware products in addition to services that may be contracted to an entity outside of the organization.

3.3.1 SA-1: System and Services Acquisition Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.2 SA-2: Allocation of Resources

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.3 SA-3: Life Cycle Support

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.
NIST SP 800-53A Control Expected Results: (1) The organization utilizes a security lifecycle methodology during development of the system. The life-cycle processes are divided into six Milestone phases: Vision & Strategy, Domain Architecture, System Architecture, System Design, System Development, and System Deployment. Security controls are embedded within each phase of the life cycle to ensure the development of secure systems and effective risk management. (2) The lifecycle is consistent with NIST Special Publication 800-64.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.4 SA-4: Acquisitions

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: (1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements has been implemented for this system.]

3.3.5 SA-5: Information System Documentation

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization ensures that adequate documentation for the information system is available, protected when required, and distributed to authorized personnel.
NIST SP 800-53 Control Enhancements: (1) The organization includes documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.
Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if

needed.
NIST SP 800-53A Control Expected Results: (1) Adequate documentation for the system is available, protected when required and distributed to the authorized personnel. The system has all the C&A documentation in accordance with organizational policy: • System Security Plan (SSP) • Security Risk Assessment (SRA) • Any Interconnection Security Agreements • Any Memorandums of Understanding • Information Technology Contingency Plan (ITCP) • Privacy Impact Assessment (PIA) • Any active Plan of Action and Milestones (POA&M) • Any active deviations • System Test and Evaluation Report • Security Assessment Report (SAR) • Executive Summary of Risk • Interim authorization to operate (IATO) or an authorization to operate (ATO) Recommendation. System utilizing security lifecycle methodology for development shall have: • Configuration Management (CM) Plan • Design Documents, • Requirements Traceability Matrix (RTM) (2) The system documentation adequately address configuration, installation, operation of the system and effectively using the system's security feature.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

3.3.6 SA-6: Software Usage Restrictions

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization complies with software usage restrictions.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.7 SA-7: User Installed Software

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization enforces explicit rules governing the downloading and installation of software by users.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.8 SA-8: Security Design Principles

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization designs and implements the information system using security engineering principles.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The system of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.
NIST SP 800-53A Control Expected Results: (1) The design of IT systems that process, store, or transmit sensitive information include, at a minimum, the technical security requirements discussed in the organizational policy. (2) Security safeguards shall be in place to ensure each person having access to sensitive IT is individually accountable for his or her actions on the system. (3) Security design principles in the development and implementation of the information systems are consistent with NIST Special Publication 800-27.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.9 SA-9: External Information System Services

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization ensures that third-party providers of outsourced information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The specific intent of this control is to address the outsourcing of job, function, or facility normally inside the organization's information system boundary. In accordance with OMB policy, an organization cannot outsource its responsibility for the security of its information systems. For commercial services that are considered commodity items (e.g., commercial telecommunications services, network services, managed security services, or system services), the organization, where feasible, specifies required security controls in available contractual vehicles and obtains the necessary assurances that the controls are in place and effective in their system. When it is infeasible to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating controls or explicitly accepts the additional risk. Third-party providers of outsourced information system services that are subject to the provisions of FISMA, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced information system

services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.
NIST SP 800-53A Control Expected Results: (1) Third-party providers are subject to the same information system security policies and procedures of the supported organization, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Requirements include: how the organization's sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor's computer systems; the background investigation and/or clearances required; any security awareness and training required for contractor activities or facilities; and any facility physical security requirements. (2) The organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.3.10 SA-11: Developer Security Testing

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system developer creates a security test and evaluation plan, implements the plan, and documents the results.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. Related security controls: CA-2, CA-4.
NIST SP 800-53A Control Expected Results: (1) The development ST&E Plan exists, document title and date are recorded. The plan was executed during system development to test the security features. (2) ST&E Plan results were documented in an ST&E Report and findings are included in a Plan of Action and Milestones.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.4 Certification and Accreditation (CA) Controls

The following section will address the controls needed for a system to be approved to operate.

3.4.1 CA-1: Certification, Accreditation, and Security Assessment Policies and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.4.2 CA-2: Security Assessments

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system. OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST Special Publication 800-53A provides guidance on security control assessments to include reuse of existing assessment results. Related security controls: CA-4, CA-6, CA-7, SA-11.
NIST SP 800-53A Control Expected Results: (1) The results from the last security control assessment are available and an assessment of the security controls in the information system is conducted [*Assignment: organization-defined period*], or when a major change occurs. (2) Security controls are

assessed for correct implementation and meet the security requirements for the system.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.4.3 CA-3: Information System Connections

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system connections on an ongoing basis. Appropriate organizational officials approve information system connection agreements.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9.
NIST SP 800-53A Control Expected Results: (1) Appropriate organizational officials have approved connections to the system and information system connection agreements (MOUs/ISAs) exist for each connection outside of the organization boundary. (2) All required MOUs/ISAs are consistent with NIST Special Publication 800-47.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.4.4 CA-4: Security Certification

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: (1) The assessment of the security controls in the information system for purposes of security certification is conducted by an independent certification agent or certification team.
Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. Related security

controls: CA-2, CA-6, SA-11.
NIST SP 800-53A Control Expected Results: (1) The previous certification documentation includes results from security control assessments, and actions taken or planned to correct deficiencies in the security controls and reduce known vulnerabilities in the system. The Certification Memo is signed by the Certifier. If the system does not have a previous certification, it will receive one during this C&A effort. Note: Certification documentation is in the process of being developed for the system's current C&A effort. This satisfies the requirement for this control. (2) The organization employs security certification process in accordance with NIST Special Publications 800-37 and 800-53A.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

3.4.5 CA-5: Plan of Action and Milestones

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops and updates [*Assignment: organization-defined frequency*], 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.
NIST SP 800-53A Control Expected Results: (1) The POA&M documents the planned, implemented, and evaluated actions to correct the deficiencies and vulnerabilities in the system identified from audits, assessments, and known vulnerabilities. (2) Deficiencies identified for future action are corrected as defined by the plan of action.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.4.6 CA-6: Security Accreditation

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.
NIST SP 800-53 Control Enhancements: None.

Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. Related security controls: CA-2, CA-4, CA-7.
NIST SP 800-53A Control Expected Results: (1) The previous accreditation documentation contains the Accreditation Memo, which is signed by the DAA. If the system does not have a previous accreditation, it will receive one during this C&A effort. Note: Accreditation documentation is in the process of being developed for the system's current C&A effort. This satisfies the requirement for this control. (2) The organization employs security accreditation process consistent with NIST Special Publications 800-37 and updates the authorization every [*Assignment: organization-defined period*] or when significant change are made to the system.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

3.4.7 CA-7: Continuous Monitoring

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization monitors the security controls in the information system on an ongoing basis.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2). This control is closely related to and mutually supportive of the activities required in monitoring

configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.
NIST SP 800-53A Control Expected Results: (1) The organization monitors the security controls in the information system on an ongoing basis. (2) The organization conducts security control monitoring in accordance with NIST Special Publication 800-37 and 800-53A.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4. OPERATIONAL CONTROLS

This section addresses operational controls, focusing on mechanisms that are primarily implemented and executed by the systems management, administration, and technical support personnel. These security controls were put in place to improve the overall security of the system environment.

4.1 Personnel Security (PS) Controls

This section describes personnel security measures used to ensure that only authorized personnel are accessing the system. To ensure secure information is not maliciously altered or unintentionally modified, System Administrators (SAs) responsible for assigning permissions should ensure that the proper permissions are granted to the proper users. All policy and procedures are followed in granting users permissions, determining permissions; ensuring user rights are restricted to the minimum necessary to perform the job, background screening and separation of duties. The subsections below further describe in greater detail the personnel security measures utilized by the system.

4.1.1 PS-1: Personnel Security Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.2 PS-2: Position Categorization

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 [*Assignment: organization-defined frequency*].
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.3 PS-3: Personnel Screening

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.4 PS-4: Personnel Termination

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.5 PS-5: Personnel Transfer

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization reviews information systems/facilities access authorizations when personnel 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).
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.6 PS-6: Access Agreements

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 and reviews/updates the agreements *[Assignment: organization defined frequency]*.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.7 PS-7: Third-Party Personnel Security

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization establishes personnel security requirements including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced systems, network and security management) and monitors provider compliance to ensure adequate security.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.1.8 PS-8: Personnel Sanctions

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2 Physical and Environmental Protection (PE) Controls

To ensure the physical and environmental protection of the system, policy and procedures have been established and implemented. This section will discuss the physical and environmental family controls as recommended by NIST SP 800-53.

4.2.1 PE-1: Physical and Environmental Protection Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.2 PE-2: Physical Access Authorizations

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops and keeps current lists of personnel with authorized access to facilities where the information system resides (except for those areas within the facility 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 [*Assignment: organization-defined frequency, at least annually*].
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.3 PE-3: Physical Access Control

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information systems resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.4 PE-5: Access Control for Display Medium

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.5 PE-6: Monitoring Physical Access

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization monitors physical access to the information systems to detect and respond to physical security incidents.
NIST SP 800-53 Control Enhancements: (1) The organization monitors real-time intrusion alarms and surveillance equipment.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.2.6 PE-7: Visitor Control

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
NIST SP 800-53 Control Enhancements: (1) The organization escorts visitors and monitors visitor activity, when required.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.2.7 PE-8: Access Records

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization maintains a visitor access records to the facility where the information system resides (except for those areas within the facility 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. Designated officials within the organization review the visitor access records at least [*Assignment: organization-defined frequency*].
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.8 PE-9: Power Equipment and Power Cabling

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization protects power equipment and power cabling for the information system from damage and destruction.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.9 PE-10: Emergency Shutoff

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: For specific locations within a facility containing concentrations of information system resources, the organization provides the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.2.10 PE-11: Emergency Power

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.2.11 PE-12: Emergency Lighting

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.12 PE-13: Fire Protection

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.
NIST SP 800-53 Control Enhancements: (1) Fire detection devices/systems activate automatically and notify the organization and emergency responders in the event of a fire. (2) Fire suppression devices/systems provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.2.13 PE-14: Temperature and Humidity Controls

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.14 PE-15: Water Damage Protection

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.15 PE-16: Delivery and Removal

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.16 PE-17: Alternate Work Site

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: Individuals within the organization employ appropriate information system security controls at alternate work sites.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.2.17 PE-18: Location of Information System Components

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3 Contingency Planning (CP) Controls

This section addresses the methods the organization uses to ensure continuity of operation of the system in the event of a disaster.

4.3.1 CP-1: Contingency Planning Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.3.2 CP-2: Contingency Plan

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: (1) 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).
NIST SP 800-53A Control Expected Results: (1) Organizational records or documents show that contingency planning policy and procedures exist and are documented, disseminated to appropriate authorized personnel, reviewed periodically by responsible parties and updated. (2) The system ITCP is developed in accordance with NIST Special Publication 800-34. (3) Organizational personnel with contingency plan implementation responsibilities understand the key elements of the contingency plan and are ready to implemented.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3.3 CP-3: Contingency Training

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].
NIST SP 800-53 Control Enhancements: None.
NIST SP 800-53A Control Expected Results: (1) The organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities. (2) Initial training is provided to individuals with responsibility implementing the system ITCP, as well as periodic refresher training. Training records include the type of contingency training received and the date completed. (3) The training material adequately addresses the activities involved with the roles and responsibilities of the contingency plan.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.3.4 CP-4: Contingency Plan Testing

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization tests the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.
NIST SP 800-53 Control Enhancements: (1) 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).
Supplemental Guidance: There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing increases with the impact level of the information system. Contingency plan testing also includes a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) arising due to contingency operations in accordance with the plan.
NIST SP 800-53A Control Expected Results: (1) The system ITCP is tested within the organization-defined frequency, and results are documented. (2) The system ITCP test results are reviewed by management after a test and the system ITCP is updated accordingly. (3) The system ITCP testing addresses the key aspects of the system ITCP. (4) Coordination took place 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) during the development of the system ITCP.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3.5 CP-5: Contingency Plan Update

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).
NIST SP 800-53A Control Expected Results: (1) The system ITCP is reviewed and updated within the organization-defined frequency. (2) During reviews, system/organizational changes or problems encountered during plan implementation, execution, or testing are considered for revisions to the plan.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.3.6 CP-6: Alternate Storage Sites

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
NIST SP 800-53 Control Enhancements: (1) The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards. (3) 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.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3.7 CP-7: Alternate Processing Sites

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable.
NIST SP 800-53 Control Enhancements: (1) The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards. (2) 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. (3) Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.
Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site.
NIST SP 800-53A Control Expected Results: (1) Agreements are in place for an alternate processing site. The alternate processing site is identified, and the date of the agreement is recorded. (2) The alternate processing site is available in accordance with the agreement. (3) The system ITCP identifies the primary processing site hazards. (4) The alternate processing site sufficiently separated from the primary site and is not susceptible to the same hazards identified at the primary site. (5) The system ITCP identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and defines explicit mitigation actions for those accessibility problems. (6) The alternate processing site agreements contain priority of service provisions in accordance with the organization's availability requirements.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3.8 CP-8: Telecommunications Services

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.
NIST SP 800-53 Control Enhancements: (1) Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements. (2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3.9 CP-9: Information System Backup

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information while in transit and at the storage location.
NIST SP 800-53 Control Enhancements: (1) The organization tests backup information within the organization-defined frequency to ensure media reliability and information integrity. (4) The organization encrypts backup information whenever the information is removed from a controlled facility and is either physically transported or electronically transmitted to another facility.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.3.10 CP-10: Information System Recovery and Reconstitution

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization employs mechanisms with supporting procedures to allow

the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, system and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.
NIST SP 800-53A Control Expected Results: (1) The organization makes available the system recovery and reconstitution procedures are documented and applied when recovery is necessary. (2) All system parameters, patches, configuration settings and system and system software are captured in a documented inventory. (3) The system is required to be tested after a recovery is completed.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4 Configuration Management (CM) Controls

This section addresses the methods the organization uses to document and control changes to the system.

4.4.1 CM-1: Configuration Management Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4.2 CM-2: Baseline Configuration

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, documents, and maintains a current, baseline configuration of the information system, an inventory of the system's constituent components, and relevant ownership information.
NIST SP 800-53 Control Enhancements: (1) The organization updates the baseline configuration of the information system and inventory of system components as an integral part of information system component installations.
Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information)

and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture. Related security controls: CM-6, CM-8.
NIST SP 800-53A Control Expected Results: (1) The system's software baseline is documented, including system source code versions, database versions, web server versions. (2) The organization maintains documented inventory of all hardware, software and firmware components that compose the information system and ownership information by component. (3) The inventory of components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture). (4) The inventory of components designates those components that are required for contingency operations. (5) The system baseline configuration is updated in accordance with NIST Special Publication 800-53A.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.4.3 CM-3: Configuration Change Control

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system. Related security controls: CM-4, CM-6, SI-2.
NIST SP 800-53A Control Expected Results: (1) A documented configuration management process exists. (2) A configuration control board (CCB) is in existence. The CCB consists of senior system management, and is responsible for reviewing and approving all requested changes to the system. The Configuration Management Plan documents the responsibilities of the CCB, as well as the members of the CCB.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4.4 CM-4: Monitoring Configuration Changes

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system. Related security control: CA-7.
NIST SP 800-53A Control Expected Results: (1) The organization monitors changes to the system and the types of changes monitored are documented. (2) A security impact analysis is performed on the system to determine how a proposed change would affect the current security posture of the system. This results of the security impact analysis are considered when making a decision to approve or disapprove the requested change.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4.5 CM-5: Access Restrictions for Change

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.
NIST SP 800-53A Control Expected Results: (1) The organization maintains a list of personnel authorized to access the system configuration or the system source code for the purpose of making changes, upgrades. (2) The ability to make configuration changes is restricted to authorized development and configuration management staff only. No system administrator, database administrator or end user staff has the ability to make configuration changes. (3) Organizational record or documents show that changes to the system are initiated by authorized personnel only.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4.6 CM-6: Configuration Settings

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems. Related security controls: CM-2, CM-3, SI-4.
NIST SP 800-53A Control Expected Results: (1) The organizational records or documents show that the system is configured as follows: (i) mandatory configuration settings for information technology products employed within the information system are established; (ii) security settings of information technology products are configured to the most restrictive mode consistent with operational requirements; (iii) configuration settings are documented; and (iv) configuration settings in all components of the information system are enforced. (2) The system configuration settings are configured in accordance with the organization-defined settings.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4.7 CM-7: Least Functionality

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*].
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.4.8 CM-8: Information System Component Inventory

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.
NIST SP 800-53 Control Enhancements: (1) The organization updates the inventory of information system components as an integral part of component installations.
Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g.,

manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.5 Maintenance (MA) Controls

This section addresses the methods the organization uses to monitor and track maintenance of the system.

4.5.1 MA-1: System Maintenance Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.5.2 MA-2: Periodic Maintenance

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: (1) 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).

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.5.3 MA-3: Maintenance Tools

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.5.4 MA-4: Remote Maintenance

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
NIST SP 800-53 Control Enhancements: (1) The organization audits all remote maintenance sessions, and appropriate organizational personnel review the maintenance records of the remote sessions. (2) The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.
Supplemental Guidance: The organization describes the use of remote diagnostic tools in the security plan for the information system. The organization maintains maintenance records for all remote maintenance, diagnostic, and service activities. Appropriate organization officials periodically review maintenance logs. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections. If password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service. For high-impact information systems, if remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems before the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.
NIST SP 800-53A Control Expected Results: (1) The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities. Telnet is not used for remote maintenance.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:

[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.5.5 MA-5: Maintenance Personnel

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: Only authorized personnel perform maintenance on the information system.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.
NIST SP 800-53A Control Expected Results: (1) Maintenance personnel have appropriate access authorizations to the system. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system. (2) The organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance personnel control is implemented.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.5.6 MA-6: Timely Maintenance

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure.
NIST SP 800-53 Control Enhancements: None.
NIST SP 800-53A Control Expected Results: (1) Maintenance support is obtained within the required time frame after an system failure.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6 System Integrity (SI) Controls

This section addresses the methods the organization uses to protect system data from accidental or malicious alteration or destruction, to provide assurance to the user that the system information meets expectations of quality and has not been altered.

4.6.1 SI-1: System and Information Integrity Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6.2 SI-2: Flaw Remediation

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization identifies, reports, and corrects information system flaws.
NIST SP 800-53 Control Enhancements: (2) The organization employs automated mechanisms to periodically and upon command demand determine the state of information system components with regard to flaw remediation.
Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring (see security controls CA-2, CA-4, or CA-7), or incident response activities (see security control IR-4) should also be addressed expeditiously. NIST Special Publication 800-40 (Version 2), provides guidance on security patch installation and patch management.
NIST SP 800-53A Control Expected Results: (1) A process is in place for identify recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the system. (2) The organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures. (3) The organization addresses flaws discovered during security assessments, continuous monitoring, or incident response. (4) The organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.6.3 SI-3: Malicious Code Protection

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system implements malicious code protection.
NIST SP 800-53 Control Enhancements: (1) The organization centrally manages virus protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms.
Supplemental Guidance: The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy

servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. Consideration is given to using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-83 provides guidance on implementing malicious code protection.
NIST SP 800-53A Control Expected Results: (1) The software automatically updates its malicious code definitions, and the definitions in use are the most current version.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.6.4 SI-4: Information System Monitoring Tools and Techniques

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.
NIST SP 800-53 Control Enhancements: (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions (e.g., the presence of malicious code) the unauthorized export of data, or signaling to an external information system).
Supplemental Guidance: Information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software, network forensic analysis tools). Monitoring devices can be strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical systems) to collect essential information. Monitoring devices can also be deployed at ad hoc locations within the system to track specific transactions (see security control AC-8 for system use notification). Additionally, these devices can be used to track the impact of security changes to the information system. The granularity of the information collected can be determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations should heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software.
NIST SP 800-53A Control Expected Results: (1) The system has intrusion detection capability. (2) The intrusion detection tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies. (3) The system is appropriately staffed and operational to monitor the information system in accordance with

organizational policy and procedures.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.6.5 SI-5: Security Alerts and Advisories

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6.6 SI-8: Spam Protection

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system implements spam protection.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6.7 SI-9: Information Input Restrictions

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization restricts the information input to the information system to authorized personnel only.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.
NIST SP 800-53A Control Expected Results: (1) The system employs restrictions on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities. (2) User accounts are restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6.8 SI-10: Information Input Accuracy, Completeness, Validity, and Authenticity

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system checks information inputs for accuracy, completeness, validity, and authenticity.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure the content is not unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, and validity of information inputs should be guided by organizational policy and operational requirements.
NIST SP 800-53A Control Expected Results: (1) The system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible. (2) The system employs rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content. (3) The system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6.9 SI-11: Error Handling

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system identifies and handles error conditions in an expeditious manner.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions should be guided by organizational policy and operational requirements.
NIST SP 800-53A Control Expected Results: (1) The system identifies and handles error conditions in expeditious manner. (2) The system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries. (3) The system provides error messages only to authorized personnel. (4) The system error logs do not contain sensitive information. (5) The system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.6.10 SI-12: Information Output Handling and Retention

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.
NIST SP 800-53 Control Enhancements: None.
NIST SP 800-53A Control Expected Results: (1) The organization retains output from the information system in accordance with organizational policy and operational requirements/procedures. (2) The organization handles output from the system according to system marked instructions and organizational policy and operational procedure and operational requirements/procedures.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.7 Media Protection (MP) Controls

To ensure the security and privacy of sensitive information, there are production, input, and output security control mechanisms, as well as sanitization procedures that provide protection of sensitive data and media. This section will discuss the media protection family controls as recommended by NIST SP 800-53 and will describe each control in place based off the criteria found in this document.

4.7.1 MP-1: Media Protection Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.7.2 MP-2: Media Access

Implementation Status: **Inherited**

NIST SP 800-53 Control: The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.
NIST SP 800-53 Control Enhancements: (1) 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.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.7.3 MP-4: Media Storage

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.7.4 MP-5: Media Transport

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization controls information system media (paper and digital) during transport and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.
NIST SP 800-53 Control Enhancements: (1) The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment: organization-defined security measures, e.g., locked container, cryptography*]. (2) The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.7.5 MP-6: Media Sanitization and Disposal

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization sanitizes information system media, both paper and digital, prior to disposal or release for reuse.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.8 Incident Response (IR) Controls

To ensure that incidents are properly reported and documented, incident response controls have been established. This section will discuss the incident response family controls as recommended by NIST SP 800-53 and will describe each control in place based off the criteria found in this document.

4.8.1 IR-1: Incident Response Policy Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.8.2 IR-2: Incident Response Training

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.8.3 IR-3: Incident Response Testing

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.8.4 IR-4: Incident Handling

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
NIST SP 800-53 Control Enhancements: (1) The organization employs automated mechanisms to support the incident handling process.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.8.5 IR-5: Incident Monitoring

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization tracks and documents information system security incidents on an ongoing basis.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.8.6 IR-6: Incident Reporting

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization promptly reports incident information to appropriate authorities.
NIST SP 800-53 Control Enhancements: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.8.7 IR-7: Incident Response Assistance

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: (1) The organization employs automated mechanisms to

increase the availability of incident response-related information and support.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

4.9 Security Awareness and Training (AT) Controls

To ensure that employees have proper security awareness and training, security policy and procedures have been established and implemented. This section will discuss the security and training family controls as recommended by NIST SP 800-53 and will describe each control in place based off the criteria found in this document.

4.9.1 AT-1: Security Awareness and Training Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.9.2 AT-2: Security Awareness

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization ensures that all users (including managers and senior executives) receive basic information system security awareness training before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.9.3 AT-3: Security Training

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

4.9.4 AT-4: Security Training Records

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5. TECHNICAL CONTROLS

This section describes the technical security mechanisms and controls that are used to minimize or prevent unauthorized users from accessing the system and to ensure its integrity, confidentiality, and availability.

5.1 Identification and Authentication (IA) Controls

Identification and Authentication (I&A) is a set of technical controls that can be used to prevent unauthorized individuals or processes from accessing the system. I&A is an important element of computer security, because it allows users to be identified and differentiated when using the system.

5.1.1 IA-1: Identification and Authentication Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.1.2 IA-2: User Identification and Authentication

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).
NIST SP 800-53 Control Enhancements: (1) The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4*] compliant.
Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in Special Publication 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and

remote information system access is NIST Special Publication 800-63 level 1 compliant. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the system level, when necessary, to provide increased information security for the organization. In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST Special Publication 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals. Related security controls: AC-14, AC-17.
NIST SP 800-53A Control Expected Results: (1) The system uniquely identifies users and authentication is accomplished through the use of passwords, tokens, or biometrics. (2) The system system configuration settings show that passwords, tokens, or biometrics corresponds to the e-authentication assurance level determined according to NIST Special Publication 800-63. (3) The system must uniquely identify and authenticate users. (4) Every user must enter a password to be authenticated to the system. (5) Every user must be uniquely identified to the system through their username.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.1.3 IA-3: Device Identification and Authentication

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system identifies and authenticates specific devices before establishing a connection.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.
NIST SP 800-53A Control Expected Results: (1) The system uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. (2) The strength of the device

authentication mechanism is consistent with FIPS 199 security categorization of the system.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.1.4 IA-4: Identifier Management

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 *[Assignment: organization-defined time period]* of inactivity; and (vi) archiving user identifiers.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.
NIST SP 800-53A Control Expected Results: (1) Each user has their own unique user name, there are no shared accounts. The user list contains an archive of current and inactive user names. (2) All system users received account access through the access authorization process. (2a) After *[organization-defined time period]* of inactivity, accounts shall be disabled from logging on, but will not be removed from the system at this time. To be reactivated, the account user shall follow prescribed procedures of the organization responsible for managing the GSS or system. (2b) After *[organization-defined time period]* of inactivity, the account password shall expire. Account shall be removed from the system or system. There will be no need to notify the account user prior to the action being taken. To gain access, the account user is required to follow access procedures requesting to be added back. (3) The organization use personal identity verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.1.5 IA-5: Authenticator Management

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-

based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
NIST SP 800-53A Control Expected Results: (1) The system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted, (ii) prohibits passwords from being displayed when entered, (iii) enforces minimum age within the organization-defined frequency, (iv) enforces maximum age within the organization-defined frequency for administrative accounts and within the organization-defined frequency for other accounts, (v) Password history shall be kept to prevent the reuse of at least organization-defined number of used passwords, (vi) Passwords shall not be reusable by the same individual for the same account for a period of organization-defined frequency. (2) (i) Passwords are provided to the end user by the system administrator through a secure mechanism that does not compromise the confidentiality of the password, (ii) This is strictly controlled and compromised passwords shall be changed promptly, (iii) Forgotten passwords are be managed following current password management procedures, (iv) Password must be changed, (iv) New users must change the password the first time they log on, (v) Passwords provided through a procedure that includes another person knowing the passwords (e.g., some help desk password resetting techniques) require the owners of the passwords to change them upon initial use when they regain access. (3) All vendor-supplied accounts and passwords, including those for software packages and maintenance accounts, are changed or disabled as soon as the system or software has been installed. (4) Sufficient safeguards are in place for identifiers and authenticators and individual authenticators are not shared or loaned and any lost or compromise is reported immediately. (5) The system establishes user control of the corresponding private key and maps the authenticated identity to the user account.
Personally Identifiable Information Mapping: OMB M-06-16, Action Item 4.1 **Personally Identifiable Information Guidance:** If policy allows PII data be accessed remotely from remote components of the system to an internal agency network, ensure the required VPN connection uses agency-controlled certificates or hardware tokens issued directly to each authorized user.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.1.6 IA-6: Authenticator Feedback

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

NIST SP 800-53A Control Expected Results: (1) When login is unsuccessful, an error message is displayed notifying the user that their login failed, but the message does not reveal information that would compromise the authentication mechanism. (2) The system does not default to displaying a password while logging on. Passwords are not displayed in clear text as they are being typed.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.1.7 IA-7: Cryptographic Module Authentication

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.
NIST SP 800-53A Control Expected Results: (1) The system encrypts authentication using a FIPS 140-2 or later validated cryptographic module. (2) Authentication methods employed by the system in accordance with FIPS 201 and NIST Special Publications 800-73 and 800-78 when the cryptographic module is a personal identity verification (PIV) card token. (3) All system authentication methods utilize the cryptographic module.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2 Access Control (AC) Controls

Logical access controls are safeguards incorporated in computer hardware, operations or systems software, and related devices to protect critical IT resources against vulnerabilities and threats from both internal and external sources. By implementing effective logical access controls, the system owner significantly reduces the risks to the system environment. The logical access controls that have been incorporated into the system include assigning access privileges, session controls, re-certification of users, encryption, networking, dial-in, object-reuse and the use of warning banners.

5.2.1 AC-1: Access Control Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated

access controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.2 AC-2: Account Management

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].
NIST SP 800-53 Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*]. (3) The information system automatically disables inactive accounts after *[organization-defined time period]*. (4) The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.
Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.
NIST SP 800-53A Control Expected Results: (1) Accounts are created through the access authorization process. (2) Each employee's manager has the primary responsibility for providing prompt notification to the responsible organization of system user status changes. The system administrator immediately suspends, cancels and/or adjusts all access privileges associated with changes in status of the user. A account deletion request is provided for each account to be removed. (3) At a minimum, an annual review of IT resources and users' accounts/profiles is performed and includes: (i) a review of the levels of access each user has, (ii) conformance with the least privilege principle, (iii) if all accounts are still active, (iv) whether management authorizations are current and, (v) if required training has been completed. (4) All accounts that have undergone modifications were done so through the access authorization process. (5) Last login-in dates for disabled accounts are prior to disabling of the account. (6) Accounts have been removed using the access authorization process and the corresponding access authorization records are available. (7) The system automatically terminates temporary and emergency accounts are after [*organization-defined time period*]. (9) Organizational records show that accounts are disabled after *[organization-defined time period]* of inactivity. (10) The system automatically disable inactive accounts after *[organization-defined time period]*.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.2.3 AC-3: Access Enforcement

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.
NIST SP 800-53 Control Enhancements: (1) The information system ensures that access to security functions (deployed in hardware, software, and firmware) and security-related information is restricted to explicitly authorized personnel (e.g., security administrators, system and network administrators, and other privileged users).
Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the system level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. Related security control: SC-13. Enhancement: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).
NIST SP 800-53A Control Expected Results: (1) The organizational records or documents show that authorization is required before a user access to the system is granted. (2) The system is access control mechanisms are configured to implement organizational access control policy. (3) The level access granted to the user are consistent with the access authorization form and only privileges that are required for the user to perform the job functions are granted. (4) The organization has explicitly defined and documented security functions for the system and grants access to security functions and information in accordance with organizational policy.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.2, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data be downloaded to a remote location, ensure access is limited to permitted information only. If policy allows PII to be remotely accessed only if not stored locally, ensure access is limited to permitted information only.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.2.4 AC-4: Information Flow Enforcement

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Related security control: SC-7.
NIST SP 800-53A Control Expected Results: (1) The agreements, if any, address permissible and impermissible flow of information and address the required level of authorization to allow information flow as defined in the information flow enforcement. (2) The system has controls in place to restrict the flow of information within the system and between interconnected system in accordance with the applicable policies, procedures, and assigned authorizations.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.2, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data be downloaded to a remote location, ensure controls are in place to permit only allowed information to be transmitted across the remote interface. If policy allows PII to be remotely accessed only if not stored locally, ensure controls are in place to permit only allowed information to be transmitted across the remote interface.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.5 AC-5: Separation of Duties

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system enforces separation of duties through assigned access authorizations.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.
NIST SP 800-53A Control Expected Results: (1) The system divides and separates duties and responsibilities of functions among different individuals so that no individual has all necessary authority and system access to disrupt or corrupt a critical security process. Access and access permissions are reviewed regularly and at least monthly. Role-Based Access Control (RBAC) concepts are implemented. (2) All functions of significant criticality or sensitivity are control by more than one individual. (3) A single user does not have the privileges to perform multiple conflicting security functions.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.6 AC-6: Least Privilege

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 specified tasks.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.
NIST SP 800-53A Control Expected Results: (1) Accounts are created with the least amount of privilege necessary to perform the user's job function. Special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or handle emergency situations. Such special privileges may be granted on a permanent or temporary basis. However, any such access is approved by a senior security manager. (2) The organization documents access rights/privileges assign to user tasks. (3) The organization documents access rights/privileges assign to user tasks.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.2, 4.4 **Personally Identifiable Information Guidance:** If PII data is accessed remotely, ensure controls are in place to enforce the most restrictive rights to the information while still allowing the individual to perform their job duties. If policy allows PII to be remotely accessed only if not stored locally, ensure controls are in place to enforce the most restrictive rights to the information while still allowing the individual to perform their job duties.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.7 AC-7: Unsuccessful Login Attempts

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to Assignment: organization-defined delay algorithm*.]] when the maximum number of unsuccessful attempts is exceeded.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.
NIST SP 800-53A Control Expected Results: (1) The system enforces maximum of [*Assignment: organization-defined number*] invalid access attempts. The system automatically locks the account for a minimum of [*Assignment: organization-defined number*] or the account shall be unlocked following current organizational procedures after [*Assignment: organization-defined number*] attempts. (2) The system enforces organizational policy and procedures for unsuccessful login attempts.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.8 AC-8: System Use Notification

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.
NIST SP 800-53A Control Expected Results: (1) The system displays a warning banner before granting access. The system use notification message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and

recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries). (2) The organization records or documents show that the system use notification message is approved.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.9 AC-11: Session Lock

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.
NIST SP 800-53A Control Expected Results: (1) The system implements and enforces a threshold for *[organization-defined time period]* before the session time-out feature is automatically invoked and requires the user to initiate a new logon.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.10 AC-12: Session Termination

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system automatically terminates a session after *[organization-defined time period]* of inactivity.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).
NIST SP 800-53A Control Expected Results: (1) The system implements and enforces a threshold for *[organization-defined time period]* of session inactivity before the session is automatically terminated.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.11 AC-13: Supervision and Review – Access Control

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.
NIST SP 800-53 Control Enhancements: (1) The organization employs automated mechanisms to facilitate the review of user activities.
Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.
NIST SP 800-53A Control Expected Results: (1) The organization supervises and reviews the activities of the users of the system. (2) The organization investigates and reports unusual activity to appropriate officials and are resolved. (3) The organizational records of supervisory notices or disciplinary actions show that the organization supervises user activities.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.2, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data be downloaded to a remote location, ensure activity logs are reviewed to maintain accountability for actions taken across remote interfaces. If policy allows PII to be remotely accessed only if not stored locally, ensure activity logs are reviewed to maintain accountability for actions taken across remote interfaces.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.2.12 AC-14: Permitted Actions without Identification or Authentication

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.
NIST SP 800-53 Control Enhancements: (1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.
Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov). Related security control: IA-2.
NIST SP 800-53A Control Expected Results: (1) The system does not permit any actions to be performed without identification and authentication of the user. (2) System configuration settings show that the organization limits specific user actions that can be performed without identification and authentication to only the actions required to accomplish mission objectives.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.2.13 AC-17: Remote Access

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, broadband, Internet) to the information system. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.
NIST SP 800-53 Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses encryption to protect the confidentiality of remote access sessions. (3) The organization controls all remote accesses through a limited number of managed access control points. (4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.1, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data be accessed remotely from remote components of the system to an internal agency network, ensure a VPN connection is required for each authorized user. If policy allows PII to be remotely accessed only if not stored locally, ensure a VPN connection is required for each authorized user.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.2.14 AC-18: Wireless Access Restrictions

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: (1) The organization uses authentication and encryption to protect wireless access to the information system.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.2.15 AC-19: Access Control for Portable and Mobile Devices

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.2.16 AC-20: Use of External Information Systems

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization restricts the use of external information systems by

authorized individuals conducting official U.S. Government business involving the processing, storage, or transmission of federal information.
NIST SP 800-53 Control Enhancements: (1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.3 Audit and Accountability (AU) Controls

This section will discuss the audit and accountability family of controls as recommended by NIST SP 800-53 and will describe each control in place based on the criteria found in this document.

5.3.1 AU-1: Audit and Accountability Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.3.2 AU-2: Auditable Events

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].
NIST SP 800-53 Control Enhancements: (3) The organization periodically reviews and updates the list of organization-defined auditable events.
Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment,

which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.
NIST SP 800-53A Control Expected Results: (1) The system generates audit records in the audit log for the following events: (a) successful log-ons and log-offs, (b) unsuccessful log-ons and log-offs, (c) change of password, (d) data files opened and closed, (e) specific actions such as reading, editing, and deleting records or fields, (f) printing reports. (2) The events are captured in the log files and contained relevant event information (i.e. Successful Logon username=Administrator).
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.2, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data be downloaded to a remote location, ensure remote audit events are recorded to maintain accountability for actions taken across remote interfaces. If policy allows PII to be remotely accessed only if not stored locally, ensure remote audit events are recorded to maintain accountability for actions taken.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.3.3 AU-3: Content of Audit Records

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: Audit records produced by or associated with the information system contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
NIST SP 800-53 Control Enhancements: (1) 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.
Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.
NIST SP 800-53A Control Expected Results: (1) Audit record content includes, for most each event captured: (i) date and time of the event; (ii) the component of the information system (e.g., software component) where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event. (2) If the system has the capability to include additional, more detailed

information in the audit records, then they should be implemented or current configuration justified.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.3.4 AU-4: Audit Storage Capacity

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.
NIST SP 800-53A Control Expected Results: (1) A sufficient amount of storage space is allocated for storage of the system's audit records and audit log is configured to prevent the audit log storage capacity from being exceeded.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.3.5 AU-5: Response to Audit Processing Failures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: In the event of an audit processing failure (e.g., software/hardware error, failure in the audit capturing mechanism, or audit storage capacity being reached), the information system alerts appropriate organizational officials and takes the following additional actions: *[Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]*.
NIST SP 800-53 Control Enhancements: None.
NIST SP 800-53A Control Expected Results: (1) An Administrator and another authorized organizational official is automatically alerted of an audit process failure via pager or e-mail.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.].

5.3.6 AU-6: Audit Monitoring, Analysis, and Reporting

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
NIST SP 800-53 Control Enhancements: (2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.
Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity

within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.
NIST SP 800-53A Control Expected Results: (1) Organizational records or documents show that the organization regular 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. (2) (i) Audit trails shall be used to review what occurred after an event, for periodic reviews, and for real-time analysis. (ii) Security Specialists shall be assigned the responsibility to review audit information including the following: (a) Audit trail review after an event; and (b) Scheduled audit reviews at least weekly or more frequently at the discretion of the information system owner. (iii) Audit tools shall allow management to hold employees accountable for user actions on computer systems.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 4.2, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data be downloaded to a remote location, ensure audit logs are reviewed to maintain accountability for actions taken across remote interfaces. If policy allows PII to be remotely accessed only if not stored locally, ensure audit logs are reviewed to maintain accountability for actions taken.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.3.7 AU-7: Audit Reduction and Report Generation

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system provides an audit reduction and report generation capability.
NIST SP 800-53 Control Enhancements: (1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.
Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.
NIST SP 800-53A Control Expected Results: (1) The system audit reduction capability is enabled and authorized users have the ability to generate reports based on the events captured in the system's audit log. (2) Automated software tools shall be used to provide audit log reduction and reporting capabilities.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.3.8 AU-8: Time Stamps

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system provides time stamps for use in audit record generation.
NIST SP 800-53 Control Enhancements: (1) The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].
Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks.
NIST SP 800-53A Control Expected Results: (1) The system is configured to include a timestamp for each event that is captured in the audit log. (2) The system log files include the exact date and time for each event that was result of an action performed at a known time. Systems administrators and network administrators shall configure organizational systems to synchronize local system clocks to the authoritative organization time server.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.3.9 AU-9: Protection of Audit Information

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.
NIST SP 800-53A Control Expected Results: (1) Only authorized system administrators with the responsibility for reviewing audit logs have access to the audit function and audit log files. No other users are allowed access in any form. (2) Only members of the system audit team have access to the system log files.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.].

5.3.10 AU-11: Audit Record Retention

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization retains audit records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
NIST SP 800-53 Control Enhancements: None.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST Special Publication 800-61 provides guidance on computer security incident handling and audit record retention.
NIST SP 800-53A Control Expected Results: (1) The system audit logs are retained for [Assignment: organization-defined number] in accordance with organizational policy, or for systems already in production, the archive contains audit log files from [Assignment: organization-defined number] prior to the current date.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4 System and Communications Protection (SC) Controls

This section will discuss the system and communications protection family of controls as recommended by NIST SP 800-53 and will describe each control in place based on the criteria found in this document.

5.4.1 SC-1: System and Communications Protection Policy and Procedures

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.2 SC-2: System Partitioning

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system separates user functionality (including user interface services) from information system management functionality.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.3 SC-4: Information Remnance

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system prevents unauthorized and unintended information transfer via shared system resources.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, or data remnants, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 3.2, 4.3, 4.4 **Personally Identifiable Information Guidance:** If policy allows PII data to be stored or downloaded to a remote site, ensure personnel receive training notifying them of the PII data encryption requirement. If policy allows PII to be remotely accessed only if not stored locally, ensure personnel receive training notifying them of the PII data handling policy.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.4 SC-5: Denial of Service Protection

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.5 SC-7: Boundary Protection

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
NIST SP 800-53 Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces. (2) The organization prevents public access into the organization's internal networks except as appropriately mediated. (3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external

telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. (5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

Implementation of Control Enhancements:
[Discuss how the NIST SP 800-53 control enhancements have been implemented for this system.]

5.4.6 SC-8: Transmission Integrity

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system protects the integrity of transmitted information.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on the Domain Name System (DNS) message authentication and integrity verification mechanisms for protection of two types of transactions (i.e., zone transfer and dynamic update).
NIST SP 800-53A Control Expected Results: (1) The system protects the integrity of transmitted information. (2) The system's web site traffic is encrypted using the HTTPS protocol.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.7 SC-9: Transmission Confidentiality

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system protects the confidentiality of transmitted information.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The FIPS 199 security category (for confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec.
NIST SP 800-53A Control Expected Results: (1) The system protects the confidentiality of transmitted information. (2) The system's web site traffic is encrypted using the HTTPS protocol.

Implementation of Control:

[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.8 SC-10: Network Disconnect

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system terminates a network connection at the end of a session or after *[organization-defined time period]* of inactivity.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The organizations applies this control within the context of risk management that considers specific mission or operational requirements; for example, when conducting, monitoring, and controlling a long-running laboratory experiment that requires continuous use of network connections.
NIST SP 800-53A Control Expected Results: (1) The system implements and enforces a threshold for *[organization-defined time period]* of session inactivity before the session is automatically terminated. (2) The system implements and enforces a threshold for *[organization-defined time period]* of session inactivity before the session is automatically terminated.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.9 SC-12: Cryptographic Key Establishment and Management

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.
NIST SP 800-53A Control Expected Results: (1) The system utilizes automated mechanisms with supporting procedures in place for digital certificate generation, installation, and distribution. Subscriber key pairs are generated and stored using FIPS 140-2 Security Level 2 or higher cryptographic modules. The same public/private key pair is not be used for both encryption and digital signature. Private keys are protected using, at a minimum, a strong password. A certificate is revoked if the associated private key is compromised; management requests revocation; or the certificate is no longer needed. (2) The system shall perform all cryptographic operations (including key generation) using FIPS 140-2 or later validated cryptographic modules operating in approved modes of operation.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.10 SC-13: Use of Cryptography

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: When cryptography is employed within the information system, the cryptography complies with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including FIPS 140-2 (as amended) which requires the system to perform all

cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: The applicable federal standard for employing cryptography in nonnational security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.
Personally Identifiable Information Mapping: OMB M-06-16, Action Items 3.1, 3.2, 4.3 **Personally Identifiable Information Guidance:** If policy allows PII data to be stored or downloaded to a remote site, provide details on the cryptography used to encrypt the PII data.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.11 SC-14: Public Access Protections

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: For publicly available information and systems, the information system protects the integrity and availability of the information and systems.
NIST SP 800-53 Control Enhancements: None.
NIST SP 800-53A Control Expected Results: (1) If the system is publicly available, the integrity of the system and its data are properly protected.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.12 SC-15: Collaborative Computing

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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).
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.13 SC-17: Public Key Infrastructure Certificates

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.14 SC-18: Mobile Code

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code.
NIST SP 800-53A Control Expected Results: (1) The organization establishes usage restrictions and implementation guidance for mobile code technologies. Mobile code usage requires authorization and are documented and monitored.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.15 SC-19: Voice Over Internet Protocol

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: 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 the use of VOIP.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.16 SC-20: Secure/Address Resolution Service (Authoritative Source)

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system (i.e., authoritative domain name system (DNS)

server) that provides name /address resolution service provides additional artifacts (i.e., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.17 SC-22: Architecture and Provisioning for Name/Address Resolution Service

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information systems that collectively provide name/address resolution service for an organization have fault tolerance and role separation.
NIST SP 800-53 Control Enhancements: None.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

5.4.18 SC-23: Session Authenticity

Implementation Status: ***[Indicate the control status as one of the following: In Place, Partially In Place, Planned, Risk Based Decision, Inherited or Not Applicable.]***

NIST SP 800-53 Control: The information system provides mechanisms to protect the authenticity of communications sessions.
NIST SP 800-53 Control Enhancements: None.
Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to ensure that session-level protection is implemented where needed, for example, for service oriented architectures providing web-based services. NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions.

Implementation of Control:
[Discuss how the NIST SP 800-53 control has been implemented for this system.]

APPENDIX A: ACRONYMS

AC	Access Controls
AT	Security Awareness and Training
ATO	Authorization to Operate
AU	Audit and Accountability
C&A	Certification & Accreditation
CCB	Configuration Control Board
CM	Configuration Management
COTS	Commercial Off the Shelf
CP	Contingency Planning
DAA	Designated Approving Authority
DR	Disaster Recovery
FIPS PUB	Federal Information Processing Standard Publications
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GOTS	Government off the shelf
GSS	General Support System
I&A	Identification and Authentication
IATO	Interim Authorization to Operate
ID	Identification
IP	Internet Protocol
IR	Incident Response
ISA	Interconnection Security Agreement
IT	Information Technology
ITCP	Information Technology Contingency Plan
MA	Maintenance
MOU	Memorandum of Understanding
MP	Media Protection
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PL	Public Law
POA&M	Plan of Action and Milestones
POC	Point of Contact
PS	Personnel Security
RA	Risk Assessment
RBAC	Role-Based Access Control
RTM	Requirements Traceability Matrix
SA	System Administrator
SC	System and Communications Protection
SDLC	System Development Life Cycle
SI	System Integrity

SORN	Systems of Records Notice
SP	Special Publication
SRA	Security Risk Assessment
SSH	Secure Shell
SSI	Security Screening Investigation
SSP	System Security Plan

APPENDIX B: REFERENCES

Laws and Regulations:

- Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347.
- Consolidated Appropriations Act of 2005, Section 522.
- USA PATRIOT Act (P.L. 107-56), October 2001.

OMB Circulars:

- OMB Circular A-130, *Management of Federal Information Resources*, November 2000.
- OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 2006.
- OMB Memorandum, M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.

FIPS Publications:

- FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

NIST Publications:

- NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems*
- NIST 800-30, *Risk Management Guide for Information Technology Systems*
- NIST 800-34, *Contingency Planning Guide for Information Technology Systems*
- NIST 800-47, *Security Guide for Interconnecting Information Technology Systems*
- NIST 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST 800-53a, *Guide for Assessing the Security Controls in Federal Information System*
- NIST 800-60, *Guide for Mapping Types of Information and Information Systems to Security*
- NIST 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*

- NIST 800-64, *Security Considerations in the Information System Development Life Cycle*.

Organization Policy and Guidance Documents:

- ***[Insert any organization business-related laws/regulations that apply to the system].***

APPENDIX C: SYSTEM/NETWORK DIAGRAM

APPENDIX D: INPUT/OUTPUT DIAGRAM

APPENDIX E: SECURITY CATEGORIZATION

[Insert Security Categorization Document]

APPENDIX F: COMBINED MEMORANDUM OF UNDERSTANDING/INTERCONNECTION SECURITY AGREEMENT(S)

[For system/systems that are interconnected with systems external to the organization, a combined "Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) document should be included here .]

If the system has no MOU/ISAs, use the following:

Since there are no interconnections between ***[Insert System Acronym]*** and systems external to the organization, no MOU/ISA is required.

APPENDIX G: RULES OF BEHAVIOR

[Insert Organizational Rules of Behavior]

APPENDIX H: E-AUTHENTICATION

Background

The e-Authentication initiative explicitly defines individual authentication as the process of establishing an understood level of confidence by which an identifier refers to a specific individual. Examples of identifiers include credentials such as Personal Identification Numbers (PINs), User IDs/passwords, tokens, or identity certificates. The e-Authentication initiative is a combination of administration and management policies, technology, credentials, agency efforts, and systems, all of which are designed to work together to reduce the paperwork burden on citizens and businesses and improve online government services for citizens. The e-Authentication Guidance for Federal Agencies, the Office of Management and Budget (OMB) memorandum M-04-04, e-Authentication Guidance for Federal Agencies, established the requirement that agencies conduct an e-Authentication risk assessment on those systems that authenticate users over a network for purposes of e-government and commerce. In addition, Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, recommends that owners of logical resources apply OMB Memorandum M-04-04 Guidance to identify the level of assurance required for their electronic transaction(s).

Guidance

The following process has been developed to assist in identifying e-Authentication systems and determining the assurance levels.

Step 1: Determine if the system falls under the purview of e-Authentication.

1. ***Does the resource/system/system require user authentication? User Authentication is defined as authentication by a "human user." For example, a user authenticates to a system by providing a username and password to gain access. The username and password serve as the authentication mechanism. Authentication focuses on confirming a person's identity, based on the reliability of his or her credential. (Yes/No)***

2. ***Does user authentication occur only through a remote access technology such as a VPN, RAS or similar technology? (Yes/No)***

3. ***Once a user is authenticated through a remote access technology, are users required to authenticate again to the resource/system/system? (Yes/No)***

If the response is "Yes" to either questions 1, 2, or 3 then the system falls under the purview of e-Authentication. Please complete the questionnaire and follow the instructions below.

However, if the response is "Yes" to question 2, the e-Authentication risk assessment should be conducted by the GSS team reviewing that specific remote access technology. Please refer

to the GSS e-Authentication risk assessment and include the assurance level and assessment summary listed in that e-Authentication report.

OR

If your response is "No" to all three questions 1, 2, and 3 your system can be categorized as not being an e-Authentication system. Please insert the following text into section 2.12 of this System Security Plan (SSP) :

> ***"[Insert System Acronym] has been determined to be a Federal System that does not require e-Authentication security controls to be implemented due to the nature of the transactions processes on the system."***

Questionnaire

Since multiple transactions may occur during the e-authentication process. Complete section A once. Complete section B of the e-Authentication Transaction questionnaire for each separate transaction. Provide the completed questionnaire to the C&A Team for a generation of an e-Authentication Assurance Profile and summary report. The summary report will be included as part of the Security Assessment Report (SAR). The C&A Team will provide text to be inserted into section 2.12.

Section A.

No.	Questions	Response			Comments
		Yes	No	N/A	
1.	Who are/will be the primary system users?				☐ Government Employees ☐ DOD Military/Citizen Employees ☐ All US Private Citizens ☐ Foreign Citizens/Governments/Companies ☐ Government Contractors ☐ Agents of US Citizens ☐ Private Business ☐ Other _____
2.	What is/are the system's network/connection entry points? **Note: Is the system/system external or internal facing?**				☐ Public Internet ☐ Internal Intranet/Extranet ☐ Direct System System Entry ☐ Public Kiosk ☐ Other _____
3.	What type of credential/authentication mechanism is used most often to authenticate users to the system?				☐ Username ☐ Password ☐ One-Time Password Device ☐ PKI ☐ Knowledge-Based ☐ Smartcard ☐ Other: _____

No.	Questions	Response			Comments
		Yes	No	N/A	
4.	What is the estimated number of electronic authentications or logins performed by the system on a daily basis?				☐ Specific Data is not collected ☐ # _____
5.	What is the system's E-Authentication Initiative Category?				☐ Government to Citizen (G2C) ☐ Government to Business (G2B) ☐ Government to Government (G2G) ☐ Internal Effectiveness and Efficiency (IEE) ☐ Other _____
6.	What is the number of unique users, in each of the designated the customer segments, that are authenticated by the system?				**G2C:** _____ **G2B:** _____ **G2G:** _____ **IEE:** _____
7.	Please identify the groups that are authenticated by the system.				☐ Business: businesses ☐ Business: employers ☐ Business: farms ☐ Business: federal contractors ☐ Business: financial institutions ☐ Business: firearms dealers ☐ Business: health care providers ☐ Business: manufacturers ☐ Business: other food industry ☐ Business: ship/boat industry
					☐ Citizen: employees ☐ Citizen: fishermen ☐ Citizen: households ☐ Citizen: individuals ☐ Citizen: landowners ☐ Citizen: retirees ☐ Citizen: students
					☐ Govt.: labor unions ☐ Govt.: law enforcement ☐ Govt.: local governments ☐ Govt.: nonprofit institutions ☐ Govt.: schools ☐ Govt.: state governments ☐ Govt.: tribal governments ☐ Govt.: universities
					☐ Internal: federal agencies ☐ Internal: federal employee beneficiaries ☐ Internal: federal employees
					☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Questions	Response			Comments
		Yes	No	N/A	
8.	What is the product from the "Approved E-Authentication Technology Provider List" being used by the system for electronic authentication purposes? **Note: The "Approved E-Authentication Technology Provider List" also specifies the version of the product that has been tested for interoperability. For the purposes of this data call, please select the appropriate product even if the version you are using is not that of the one on the list.**				☐ Entegrity AssureAccess v3.0.0.4 ☐ Entrust GetAccess v7.0 SP 2 Patch 3 ☐ Hewlett-Packard Select Access v5.2 ☐ IBM Tivoli Federated Identity manager v5.1.1 ☐ Oblix ShareID 2.0 ☐ RSA Security Federal Identity Manager v2.5LA ☐ Sun Microsystems Sun Java System Identity Server v6.1 ☐ Netegrity Site Minder 6.0.1.04 ☐ Trustgenix IdentityBridge 2.1 ☐ Databases ☐ COTS Product: Please specify: _____ ☐ Operating System ☐ Other: _____

Section B.

9.	Please provide the Transaction Name.				_____
10.	What is the Transaction Type?				☐ Inquire ☐ Create ☐ Modify ☐ Delete
11.	What is the data associated with this transaction?				☐ Audit Thresholds ☐ Cryptographic Keys ☐ Electronic Mail ☐ Employee Record ☐ Firewall Configuration Settings ☐ Incident Reports ☐ Operating System Executables ☐ Personal Profile ☐ Business Profile ☐ Web Page ☐ Financial ☐ Other: _____ ☐ Other: _____
12.	Describe the data associated with this transaction. **Note: If applicable, select from the following security requirements associated with the data.**				_____ _____ ☐ Confidentiality ☐ Integrity ☐ Availability ☐ Privacy ☐ Pseudonimity ☐ Anonymity ☐ Nonrepudiation

13.	Who is the transaction user?				☐ Agents of US Citizens ☐ All US Private Citizens ☐ DOD Citizen Employees ☐ DOD Military ☐ Foreign Citizens/Governments/Companies ☐ General Public ☐ Government Contractors ☐ Government Employees ☐ Other: _____
14.	What is the entry point, the instrumental vehicle for the transaction? (e.g., Internet, registered user portal, employee user portal, intranet, extranet).				☐ Internet ☐ Intranet ☐ Other: _____
15.	What is the transaction security context? **Note: Definitions of the transaction security contexts:** ▪ **Recurring Transaction – Regular or periodic transactions between parties have a higher risk than intermittent transactions because of their predictability, causing a higher likelihood that an outside party would know of the scheduled transaction and prepare to intrude on it.** ▪ **High-value Transaction – The value of the information to outside parties could also determine their motivation to compromise the information. Information relatively unimportant to an agency may have a high value to an outside party.** ▪ **Mission-Specific Transaction – Certain agencies, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction. The act of disruption can be an end in itself.**				☐ Recurring Transaction ☐ High-Value Transaction ☐ Mission-Specific Transaction ☐ N/A

16.	What is the security context of the information that is generated or carried via the transaction? **Note: Definitions of the action security contexts:** ▪ **Archival – Will be archived later as permanently valuable records;** ▪ **Auditable – May later be subject to audit or compliance;** ▪ **Forensic – May later be needed as proof in court;** ▪ **Nonvolatile – Will be used for a long time prior to being discarded;** ▪ **Research-related – Will be used for research, program evaluation, or other statistical analyses;** ▪ **Subject to Dispute – May later be subject to dispute by one of the parties (or alleged parties) to the transaction; and** ▪ **Subject to Nonparty Dispute – May later be subject to challenge by a nonparty to the transaction.**				☐ Archival ☐ Auditable ☐ Forensic ☐ Nonvolatile ☐ Research-related ☐ Subject to Dispute ☐ Subject to Nonparty Dispute
17.	What is the data type (categorization) for this transaction?				The data type for this transaction is:
18.	What are the sensitivity ratings for this data type? **Note: This is the final security categorization ratings.**				**Confidentiality (C)** ☐ Low ☐ Moderate ☐ High **Integrity (I)** ☐ Low ☐ Moderate ☐ High **Availability (A)** ☐ Low ☐ Moderate ☐ High

19.	Are there possible Impact Areas for the system? **Note: Main impact areas are defined from which an identity authentication error would impact negatively. If there are no possible Impact Areas for the system and the answer is "No," the questionnaire is complete. If the answer is "Yes," please specify and proceed to the next question.**	☐	☐	☐	
20.	What are the possible Impact Areas for the system and the maximum level of impact resulting from authentication failure associated? **Note: Main impact areas are defined from which an identity authentication error would impact negatively.** **Note: For precise criteria of level of impact resulting from authentication failure please refer to Exhibit A.**				☐ AC1 – Inconvenience, distress or damage to standing or reputation ☐ Low ☐ Moderate ☐ High ☐ AC2 – Financial loss or agency liability ☐ Low ☐ Moderate ☐ High ☐ AC3 – Harm to agency programs or public interests ☐ Low ☐ Moderate ☐ High ☐ N/A ☐ AC4 – Unauthorized release of sensitive information ☐ Low ☐ Moderate ☐ High ☐ N/A ☐ AC5 – Personal Safety ☐ Low ☐ Moderate ☐ High ☐ N/A ☐ AC6 – Civil or criminal violations ☐ Low ☐ Moderate ☐ High ☐ N/A

Exhibit A: Potential Impact of Authentication Failures

Potential Impact Categories	Impact		
	Low	**Moderate**	**High**
Inconvenience, distress, or damage to standing or reputation	At worst, limited, short-term inconvenience, distress or embarrassment to any party	At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	Severe or serous long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals)
Financial Loss or agency liability	At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability	At worst, a serious unrecoverable financial loss to any party, or serious agency liability	Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability
Harm to agency programs or public interests	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness, or (ii) minor damage to organizational assets or public interest	At worst, a serious adverse effect on organizational operation or assets, or public interest. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness, or (ii) significant damage to organizational assets or public interest	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation to the extent and duration that the organization unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interest
Unauthorized release of sensitive information	At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a moderate impact as defined in FIPS PUB 199	A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199
Personal safety	At worst, minor injury not requiring medical treatment	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment	A risk of serious injury or death
Civil or criminal violations	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement effects	At worst, a risk of civil or criminal violations that may be subject to enforcement effects	A risk of civil or criminal violations that are of special importance to enforcement programs

APPENDIX I: PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

[Insert PIA Questionnaire after final approval.]

APPENDIX J: SSP CONTROL IMPLEMENTATION SUMMARY

[Insert an 'X' for the appropriate status for each control selected for the system.]

Control	In Place	Partially in Place	Planned	Risk Based Decision	Inherited		Not Applicable
					Organizational	GSS	
RA-1							
RA-2							
RA-3							
RA-4							
RA-5							
PL-1							
PL-2							
PL-3							
PL-4							
PL-5							
PL-6							
SA-1							
SA-2							
SA-3							
SA-4							
SA-5							
SA-6							
SA-7							
SA-8							
SA-9							
SA-11							
CA-1							
CA-2							
CA-3							
CA-4							
CA-5							
CA-6							
CA-7							
PS-1							
PS-2							
PS-3							
PS-4							
PS-5							
PS-6							
PS-7							
PS-8							
PE-1							
PE-2							
PE-3							
PE-5							
PE-6							
PE-7							
PE-8							
PE-9							
PE-10							

Control	In Place	Partially in Place	Planned	Risk Based Decision	Inherited		Not Applicable
					Organizational	GSS	
PE-11							
PE-12							
PE-13							
PE-14							
PE-15							
PE-16							
PE-17							
PE-18							
CP-1							
CP-2							
CP-3							
CP-4							
CP-5							
CP-6							
CP-7							
CP-8							
CP-9							
CP-10							
CM-1							
CM-2							
CM-3							
CM-4							
CM-5							
CM-6							
CM-7							
CM-8							
MA-1							
MA-2							
MA-3							
MA-4							
MA-5							
MA-6							
SI-1							
SI-2							
SI-3							
SI-4							
SI-5							
SI-8							
SI-9							
SI-10							
SI-11							
SI-12							
MP-1							
MP-2							
MP-3							
MP-4							
MP-5							
MP-6							
IR-1							
IR-2							
IR-3							
IR-4							

Control	In Place	Partially in Place	Planned	Risk Based Decision	Inherited		Not Applicable
					Organizational	GSS	
IR-5							
IR-6							
IR-7							
AT-1							
AT-2							
AT-3							
AT-4							
IA-1							
IA-2							
IA-3							
IA-4							
IA-5							
IA-6							
IA-7							
AC-1							
AC-2							
AC-3							
AC-4							
AC-5							
AC-6							
AC-7							
AC-8							
AC-11							
AC-12							
AC-13							
AC-14							
AC-17							
AC-18							
AC-19							
AC-20							
AU-1							
AU-2							
AU-3							
AU-4							
AU-5							
AU-6							
AU-7							
AU-8							
AU-9							
AU-11							
SC-1							
SC-2							
SC-4							
SC-5							
SC-7							
SC-8							
SC-9							
SC-10							
SC-12							
SC-13							
SC-14							
SC-15							

Control	In Place	Partially in Place	Planned	Risk Based Decision	Inherited		Not Applicable
					Organizational	GSS	
SC-17							
SC-18							
SC-19							
SC-20							
SC-22							
SC-23							

APPENDIX K: ROLES AND RESPONSIBILITIES

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
RA-2: Security Categorization		Responsible for ensuring that the system has been categorized in accordance with FIPS 199 and documenting the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.
RA-3: Risk Assessment		Responsible for ensuring that risk assessments are being performed on the system [*Assignment: organization-defined period*] or whenever a significant change has been made to the system.
RA-4: Risk Assessment Update		Responsible for ensuring risk assessments are being updated in accordance with organizational policy.
RA-5 Vulnerability Scanning		Run and analyze vulnerability scans on system. This is identified in the system SSP in section 3.1.5.
PL-2: System Security Plan		Responsible for disseminating the System Security Plan (SSP) to appropriate elements within the organization and assigning responsibilities to specific parties and defining specific actions to ensure that the SSP control is being properly implemented. In addition, ensures that Designated officials within the organization review and approve the plan.
PL-3: System Security Plan Update		Responsible for reviewing the security plan for the system [*Assignment: organization-defined period*] or when significant changes are made to the system and revising the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
PL-5: Privacy Impact Assessment		Responsible for ensuring that a privacy impact assessment on the information system has been conducted.
PL-6: Security-Related Activity Planning		Responsible for ensuring that appropriate planning and coordination occur before conducting security-related activities affecting the system in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.
SA-3: Life Cycle Support		Responsible for managing the information system using the system development life cycle or other approved methodology that includes information security considerations.
SA-5: Information System Documentation		Responsible for ensuring documentation of the system is captured and maintained.
SA-8: Security Engineering Principles		Responsible for ensuring that the design of the system includes, at a minimum, the technical security requirements discussed in organizational policy. In addition ensures that security design principles in the development and implementation of the system are consistent with NIST Special Publication 800-27.

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
SA-9: External Information System Services		Responsible for ensuring that third-party providers of outsourced information system services employ security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. In addition, monitors outsourced information system services for indications of inappropriate or unusual activity.
SA-11: Developer Security Testing		Responsible for ensuring that a development ST&E Test Plan is developed, executed and the results are documented.
CA-2: Security Assessments		Responsible for ensuring that assessments of the security controls of the system are assessed [*Assignment: organization-defined period*] 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.
CA-3: Information System Connections		Responsible for authorizing all connections from the system to other information systems outside of the accreditation boundary and monitors/controls the system connections on an ongoing basis. Appropriate organizational officials approve information system connection agreements.
CA-4: Security Certification		Responsible for ensuring that the certification of the system is conducted by an independent certification agent and that the certification process is NIST SP 800-37, and 800-53A compliant.
CA-5: Plan of Action and Milestones		Responsible for developing and updating [*Assignment: organization-defined period*], 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.
CA-6: Security Accreditation		Responsible for authorizing (i.e., accredits) the system for processing before operations and updates the authorization [*Assignment: organization-defined period*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.
CA-7: Continuous Monitoring		Responsible for ensuring that security controls of the system are monitored on an ongoing basis.
CP-2: Contingency Plan		Responsible for coordinating the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan) and ensures that key operating elements within the organization understand the contingency plan and are ready to implement the plan.
CP-3: Contingency Training		Responsible for coordinating contingency plan testing and ensuring that training is conducted on the contingency plan.
CP-4: Contingency Plan Testing		Responsible for coordinating 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).

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
CP-5: Contingency Plan Update		Responsible for reviewing the contingency plan for the information system [*Assignment: organization-defined period*] and revising the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
CP-7: Alternate Processing Sites		Responsible for identifying an alternate processing site and initiating necessary agreements to permit the resumption of information system operations for critical mission/business functions within specified time period when the primary processing capabilities are unavailable.
CP-10: Information System Recovery and Reconstitution		Responsible for ensuring that system recovery and reconstitution procedures are documented and applied when recovery is necessary.
CM-2: Baseline Configuration and System Component Inventory		Responsible for developing, documenting, and maintaining a current, baseline configuration of the information system, an inventory of the system's constituent components, and relevant ownership information.
CM-3: Configuration Change Control		Responsible for documenting control changes to the system. In addition, appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.
CM-4: Monitoring Configuration Changes		Responsible for monitoring changes to the system and for having security impact analyses conducted to determine the effects of the changes.
CM-5: Access Restrictions for Change		Responsible for establishing mandatory configuration settings for information technology products employed within the system; (ii) and configuring the security settings of information technology products to the most restrictive mode consistent with system operational requirements; (iii) and documenting the configuration settings; and (iv) enforcing the configuration settings in all components of the information system.
CM-6: Configuration Settings		Responsible for ensuring that the system is configured to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services.
CM-7: Least Functionality		Responsible for ensuring that the system provides only the essential capabilities and prohibits any functionality that is not essential.
MA-2: Periodic Maintenance		Responsible for ensuring that routine preventative and regular maintenance on the components of the system are scheduled, performed, and documented in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-3: Maintenance Tools		Responsible for approving, controlling, and monitoring the use of system maintenance tools and ensuring that the tools are maintained on an ongoing basis.
MA-4: Remote		Responsible for approving, controlling, and monitoring remotely executed

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
Maintenance		maintenance and diagnostic activities.
MA-5: Maintenance Personnel		Responsible for maintaining a list of personnel that have appropriate access authorizations to the system.
MA-6: Timely Maintenance		Responsible for maintaining support agreements and ensures that the inventory of spare parts is sufficient to support the system.
SI-2: Flaw Remediation		Responsible for ensuring that newly released security patches, service packs, and hot fixes for the system are tested and implemented within a reasonable timeframe.
SI-3: Malicious Code Protection		Responsible for ensuring that malicious code protection mechanisms for protecting against malicious code (e.g., file transfer software, instant messaging software) have been implemented on the system.
SI-4: Information System Monitoring Tools and Techniques		Responsible for ensuring that information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools have been implemented for protecting the system.
SI-9: Information Input Restrictions		Responsible for ensuring that restrictions are employed on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities.
SI-10: Information Accuracy, Completeness, Validity, and Authenticity		Responsible for ensuring that the information accuracy, completeness, validity and authenticity control is properly implemented.
SI-11: Error Handling		Responsible for ensuring that the system is properly performing error handling.
SI-12: Information Output Handling and Retention		Responsible for ensuring that output from the system in handled in accordance with organizational policy which includes proper marking, distribution, and disposal.
IA-2: User Identification and Authentication		Responsible for ensuring that the system uniquely identifies and authenticates users (or processes acting on behalf of users).
IA-3: Device Identification and Authentication		Responsible for ensuring that the system uses either shared known information or an organizational authentication solution to identify and authenticate devices on local and/or wide area networks.
IA-4: Identifier Management		Responsible for managing user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) ensuring that authorizations are received from an appropriate organization official prior to a user being issued an identifier on the system; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after *[organization-defined time period]* of inactivity; and (vi) archiving user identifiers.

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
IA-5: Authenticator Management		Responsible for the ensuring that the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, and that the system enforces minimum age, enforces maximum age of *[organization-defined time period]* for administrative accounts and *[organization-defined time period]* for other account, that password history is maintained by the system which prevents the reuse of [*Assignment: organization-defined period*] used passwords, and that passwords are not reusable by the same individual for the same account on the system for a period of [*Assignment: organization-defined period*].
IA-6: Authenticator Feedback		Responsible for ensuring that the authenticator feedback (e.g., password characters not being displayed during login) control is properly implemented.
IA-7: Cryptographic Module Authentication		Responsible for ensuring that system encrypts authentication data using a FIPS 140-2 or later validated cryptographic module.
AC-2: Account Management		Responsible for ensuring that new user accounts are only created after the user has completed the account management process. In addition, conducts system account reviews [*Assignment: organization-defined period*]; and ensures that inactive accounts are disabled after *[organization-defined time period]* days and removed after *[organization-defined time period]* days.
AC-3: Access Enforcement		Responsible for ensuring that authorization is required before a user is granted access to the system and defines security functions for the system and ensures that access is granted in accordance with organizational security policy.
AC-4: Information Flow Enforcement		Responsible for ensuring that the system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
AC-5:Separation of Duties		Responsible for ensuring that separation of duties is implemented and enforced and that personnel with duties requiring the use of the system.
AC-6: Least Privilege		Responsible for ensuring that the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks are assigned.
AC-7: Unsuccessful Login Attempts		Responsible for ensuring that the system is configured to enforce: the maximum number of consecutive invalid access attempts within a certain period of time; a limit of [*Assignment: organization-defined period*] invalid access attempts by a user during; automatic locks for a minimum of [*Assignment: organization-defined period*] or the account shall be unlocked following current password management procedures after [*Assignment: organization-defined period*] attempts.
AC-8: System Use Notification		Responsible for ensuring that a warning banner in compliance with organizational policy is being displayed on the system prior to being able to login.
AC-11: Session Lock		Responsible for ensuring that the system is configured to initiate a session lock until the user re-establishes access using appropriate identification and

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
		authentication procedures.
AC-12: Session Termination		Responsible for ensuring that the system is configured to automatically terminate a session after *[organization-defined time period]* of inactivity.
AC-13: Supervision and Review		Responsible for supervising and reviewing the activities of users with respect to the enforcement and usage of information system access controls.
AC-14: Permitted Actions without Identification or Authentication		Responsible for ensuring that specific user actions that can be performed without identification and authentication are limited to only those actions required to accomplish mission objectives.
AC-19: Access Control for portable and mobile systems		Responsible for establishing 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.
AU-2: Auditable Events		Responsible for ensuring the system is configured so that auditing is enabled and that it is capturing security significant events.
AU-3: Content of Audit Records		Responsible for ensuring that the system includes the capability to include detailed information in audit records/logs.
AU-4: Audit Storage Capacity		Responsible for ensuring that the system allocates sufficient audit record storage capacity and establishing configuration settings to prevent such capacity from being exceeded.
AU-5: Response to Audit Processing Failures		Responsible for ensuring that in the event of an audit failure or audit storage capacity being reached, the system alerts appropriate organizational officials and takes any additional organization-defined actions.
AU-6: Audit Monitoring, Analysis, and Reporting		Responsible for regularly reviewing/analyzing system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
AU-7: Audit Reduction and Report Generation		Responsible for ensuring that the system provides an audit reduction and report generation capability and that it is configured correctly.
AU-8: Time Stamps		Responsible for ensuring that the system is configured to provide time stamps for use in audit record generation.
AU-9: Protection of Audit Information		Responsible for ensuring that the system protects audit information and audit tools from unauthorized access, modification, and deletion.
AU-11: Audit Record		Responsible for ensuring audit records for the system are maintained for [*Assignment: organization-defined period*] to provide support for after-the-fact

SECURITY CONTROL	RESPONSIBLE PARTY/ NAME & TITLE	RESPONSIBILITY
Retention		investigations of security incidents and to meet regulatory and organizational information retention requirements.
SC-2: System Partitioning		Responsible for ensuring that the system physically and/or logically separates user functionality (including user interface services) from information system management functionality and how the separation is implemented and enforced.
SC-4: Information Remnance		Responsible for ensuring that the system prevents unauthorized and unintended information transfer via shared system resources.
SC-8: Transmission Integrity		Responsible for ensuring that the system protects the integrity of transmitted information.
SC-9: Transmission Confidentiality		Responsible for ensuring that the system protects the confidentiality of transmitted information.
SC-10: Network Disconnect		Responsible for ensuring that the system terminates a network connection at the end of a session or after *[organization-defined time period]* of inactivity.
SC-12: Cryptographic Key Establishment and Management		Responsible for ensuring that the system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and management and how the mechanisms and procedures are implemented.
SC-13: Use of Validated Cryptography		Responsible for ensuring that the employed cryptography (e.g., SC-12) complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.
SC-14: Public Access Protections		Responsible for ensuring that for Publicly available systems the system protects the integrity of the information and systems and how the protections are implemented.
SC-15: Collaborative Computing		Responsible for ensuring that the Collaborative Computing control is properly implemented.
SC-18: Mobile Code		Responsible for establishing usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; documenting, monitoring, and controlling the use of mobile code within the information system; and for ensuring that authorized officials approve the use of mobile code.
SC-23: Session Authenticity		Responsible for ensuring that the system provides mechanisms to protect the authenticity of communications sessions.

ADDENDUM 1: SYSTEM/DOCUMENT CHANGE RECORDS

OMB Circular A-130 requires that system security plans be continuously updated to reflect the current design and security posture of the system. This addendum to the system security plan is designed and completed to satisfy the OMB requirement. The system changes provided within this addendum must be incorporated into the security plan every [*Assignment: organization-defined period*] during the system's re-accreditation or when the system change is significant to completely invalidate the current security plan.

Change/Review Control Log			
Name of Change	**Date of Change**	**Date of Review**	**Authorized By**