Annual Self-Assessment Template Completion Guidance

Template last updated on: March 6, 2014

The annual self-assessment template was developed to support FIPS 199 categorization for **MODERATE** impact systems. The controls in the template are compliant with the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 Revision 4, including errata changes through April 2013.

Disclaimer: As of the date this template was revised; NIST has not yet issued a final NIST Special Publication 800-53A associated with the Revision 4 controls. Consequently, the column that describes *NIST 800-53A Assessment Steps Used* may be outdated.

Information System Security Officers (ISSOs) may conduct their 2014 annual self assessments using NIST Special Publication 800-53 Revision 3 controls. ISSOs are encouraged, however, to use the NIST 800-53 Revision 4 template.

Assessment of Controls:

ISSOs need not assess "common" controls, nor do they need to assess the common portion of a "hybrid" control. ISSOs should focus their review on "system-specific" controls and the system-specific portion of a "hybrid" control. The ISSO is responsible for determining whether a control is actually common, system-specific or hybrid for the given application/system under review.

Note: For systems external to Federal Student Aid general support system (VDC) - the general support system common controls need to be evaluated as part of the annual self assessment.

PRA Burden Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. The valid OMB control number for this information collection is 1845-XXXX. Public reporting burden for this collection of information is estimated to average 316 hours per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The obligation to respond to this collection is mandatory (428(c) of the Higher Education Act of 1965, as amended). If you have comments or concerns regarding the status of your individual submission of this form/application/survey, please contact the FSA Technology Office at FSA_GAsecurity@ed.gov directly.

Assessment Template Column Descriptions		
Column Name	**Field Completion Instructions**	**Description**
Security Control Information		
NIST Security Control Number	No updates required	NIST SP 800-53 Revision 4 Control ID
Security Control Name	No updates required	Name of security control
Priority / Baseline Allocation	No updates required	The NIST designated priority codes: P0, P1, P2 or P3 and the baseline allocation for the appropriate system categorization. NIST recommends using the priority codes when making sequencing decisions on control implementations. Baseline allocation is the minimum set of security controls and associated enhancements that should be implemented for a given categorization.
Security Control and Enhancements	No updates required	Describes the security controls and the enhancements that are applicable at the template's specified categorization. These are pulled directly from NIST SP 800-53 Revision 4.
Security Control Type	Verified by Assessor / ISSO	Identifies whether the control is common, hybrid, system level or not applicable. Any controls that are generally common for systems at the VDC are marked as such in the template, however this type should always be verified by the ISSO.
Control Assessment Information		
Last Date Security Control Assessed	Entered by Assessor	Last date the control was assessed - either by self-assessment or security authorization (SA)
Assessor Information	Entered by Assessor	Documents the assessor name, role and email

Control Assessment Information		
Assessed Security Control Effectiveness	Entered by Assessor	Choose from the following: 1. **Satisfied:** Control is implemented and operating effectively, no issue founds 2. **Partially satisfied**: Part of the control is met, but some issues were found; issues found described in "Findings/Deficiencies Found" column 3. **Not satisfied**: The control is not implemented or operating effectively; issues found described in "Findings/Deficiencies Found" column 4. **Not applicable**: The control is not applicable to this system; justification for status included in "Scoping Guidance/Risk Based Decision Justification" column. 5. **Risk-based decision not to implement**: The control was not implemented due to a risk-based decision; details on OVMS ID and Accepted Risk documentation developed included in "Scoping Guidance/Risk Based Decision Justification" column.
Findings / Deficiencies Found	Entered by Assessor	Describes the issues found when assessing the control. Should list details of issues found in sampling, scans, documentation or screen shots.
Scoping Guidance / Risk Based Decision Justification	Entered by Assessor	Describes the justification for the control being identified as not applicable or the justififcation that was made for the control to not be implemented based on a risk-based decision. Risk based decisions should be supported by Accepted Risk documentation.
NIST 800-53A Assessment Steps Used	Modified by Assessor if additional steps used	Lists the assessment steps to be used to verify the imlementation status and implementation effectiveiness of each control. Verbiage is pulled from latest version (as of template last update date) of NIST SP 800-53 A.
Assessment Evidence	Entered by Assessor	Describes the evidence gathered and reviewed by the assessor in testing the control. Assessor should include: 1. Any documentation or scans reviewed, such as the SSP, procedures or Qualys scans 2. Description of samples obtained, such as review of a user account creation to verify following procedures 3. Description of any screen shots, such as screen shots obtained after testing audit log contents

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1 MOD AC-1	Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-1.1 Examine organizational records or documents to determine if access control policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. AC-1.2 Examine the access control policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. AC-1.3 Examine the access control procedures to determine if the procedures are sufficient to address all areas identified in the access control policy and all associated access controls. AC-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control policy and procedures control is implemented.	
AC-2	ACCOUNT MANAGEMENT	P1 MOD AC-2 (1) (2) (3) (4)	Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-2.1 Examine organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures. AC-2.2 Examine organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures. AC-2.3 Examine selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation. AC-2.4 Examine a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled. AC-2.5 Examine a list of recently separated or terminated employees to determine if the organization removed accounts for these individuals according to established procedures and completed any organization-required documentation. AC-2.6 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.	
AC-2	ACCOUNT MANAGEMENT	P1 MOD AC-2 (1) (2) (3) (4)	Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically [Selection: removes; disables] temporary and emergency accounts after [ASSIGNMENT: organization-defined time period for each type of account]. (3) The information system automatically disables inactive accounts after [ASSIGNMENT: organization defined time period]. (4) The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [ASSIGNMENT: organization-defined personnel or roles].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			Control Enhancements: AC-2(1) Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented. AC-2(2) Examine organizational records or documents to determine if temporary and emergency accounts are automatically terminated after [organization defined time period] for each type of account. AC-2(3) Examine organizational records or documents to determine if inactive accounts on the information system are automatically disabled after [organization-defined time period]. AC-2(4) Examine the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after [organization-defined time period].	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-3	ACCESS ENFORCEMENT	P1 LOW AC-3	Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-3.1 Examine organizational records or documents to determine if user access to the information system is authorized AC-3.2 Examine access control mechanisms to determine if the information system is configured to implement the organizational access control policy. AC-3.3 Examine the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations. AC-3.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented. AC-3.7 Examine organizational records or documents to determine if the organization explicitly defines security functions for the information system. AC-3.8 Examine organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy.	
AC-4	INFORMATION FLOW ENFORCEMENT	P1 MOD AC-4	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [ASSIGNMENT: organization-defined information flow control policies].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-4.1 Examine information system interconnection agreements to determine if the agreements address: (i) the types of permissible and impermissible flow of information between systems; and (ii) the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures. AC-4.2 Examine information system configuration settings to determine if controls are in place to restrict the flow of information within the system and between interconnected systems in accordance with the applicable policy, procedures, and assigned authorizations. AC-4.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information flow enforcement control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-5	SEPARATION OF DUTIES	P1 MOD AC-5	Control: The organization: a. Separates [ASSIGNMENT: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-5.1 Examine organizational records or documents to determine if the information system enforces separation of duties. AC-5.2 Examine organizational records or documents to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual. AC-5.3 Examine selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions). AC-5.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.	
AC-6	LEAST PRIVILEGE	P1 MOD AC-6 (1) (2)	Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancements: (1) The organization explicitly authorizes access to [ASSIGNMENT: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information]. (2) The organization requires that users of information system accounts, or roles, with access to [ASSIGNMENT: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing nonsecurity functions.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			Control Enhancements: AC-6(1) Examine organizational records or documents to determine if: (i) the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; and (ii) the organization explicitly authorizes access to the organization-defined security functions and security-relevant information. AC-6(2) Examine organizational records or documents to determine if: (i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access; and (ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions; and (iii) the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions. AC-6(3) Examine organizational records or documents to determine if (i) the organization defines the privileged commands to which network access is to be authorized only for compelling operational needs; (ii) the organization authorizes network access to organization-defined privileged commands only for compelling	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2 MOD AC-7	Control: The information system: a. Enforces a limit of [ASSIGNMENT: organization-defined number] consecutive invalid access attempts by a user during a [ASSIGNMENT: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [ASSIGNMENT: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [ASSIGNMENT: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	Common, Hybrid IF SYSTEM USES AIMS, COMMON. IF SYSTEM USES PIN, MAY ALSO BE COMMON (if PIN outside of boundaries). ELSE HYBRID (system specific, but VDC provided for "backend" accounts). This common control is provided by the VDC.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-7.1 Examine organizational records or documents to determine if the information system in accordance with access control policy and procedures: (i) enforces the maximum number of consecutive invalid access attempts within a certain period of time; (ii) automatically enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period; and (iii) enforces automatic locks on the account/node for an organization-defined time period or delays the next login prompt according to an organization defined delay algorithm when the maximum number of unsuccessful attempts is exceeded AC-7.2 Examine the information system configuration settings to determine if the information system enforces organizational policy and procedures for unsuccessful login attempts. AC-7.3 Test the account lockout policy on selected user accounts by exceeding the maximum number of invalid login attempts within the organization-defined time period on the information system to determine if the information system locks the account/node. AC-7.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the unsuccessful login attempts control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-8	SYSTEM USE NOTIFICATION	P1 MOD AC-8	Control: The information system: a. Displays to users[ASSIGNMENT: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [ASSIGNMENT: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.	Common, Hybrid IF SYSTEM USES AIMS, COMMON. IF SYSTEM USES PIN, MAY ALSO BE COMMON (if PIN outside of boundaries). ELSE HYBRID (system specific, but VDC provided for "backend" accounts).			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-8.1 Examine the information system use notification message to determine if the 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). AC-8.2 Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use. AC-8.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.	
AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	NOT SELECTED	Not Selected								
AC-10	CONCURRENT SESSION CONTROL	SELECTED FOR HIGH ONLY	Control: The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement				
AC-11	SESSION LOCK	P3 MOD AC-11	Control: The information system: c. Prevents further access to the system by initiating a session lock after [ASSIGNMENT: organization-defined time period] of inactivity or upon receiving a request from a user; and d. Retains the session lock until the user reestablishes access using established identification and authentication procedures. Control Enhancements: (1) The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Common, Hrbyrid IF SYSTEM USES AIMS, COMMON. IF SYSTEM USES PIN, MAY ALSO BE COMMON (if PIN outside of boundaries). ELSE HYBRID (system specific, but VDC provided for "backend" accounts).			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-11.1 Examine the configuration settings of the information system to determine if the system initiates a session lock until the user reestablishes access using appropriate identification and authentication procedures. AC-11.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the session lock control is implemented.	
AC-12	SESSION TERMINATION	P2 MOD AC-12	Control: The information system automatically terminates a user session after [ASSIGNMENT: organization-defined conditions or trigger events requiring session disconnect].	Hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-12 Examine the information system configuration settings to determine if the information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	P1 MOD AC-14	Control: The organization: a. Identifies [ASSIGNMENT: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-14.1 Examine organizational records or documents to determine what specific user actions can be performed on the information system without requiring identification and authentication. AC-14.2 Examine the configuration settings of the information system to determine if the system allows users to perform certain actions on the system without identifying and authenticating to the system in accordance with access control policy and procedures. AC-14.3 Test the information system by attempting to perform actions that are permitted without identification and authorization to determine if those actions can be performed in accordance with access control policy and procedures. AC-14.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the permitted actions without identification and authentication control is implemented. AC-14.8 Examine organizational records or documents to determine if the organization limits specific user actions that can be performed without identification and authentication to only the actions required to accomplish mission objectives. AC-14.9 Examine the configuration settings of the information system to determine if the system allows users to perform certain mission related actions without identifying and authenticating to the system.	
AC-16	SECURITY ATTRIBUTES	NOT SELECTED	Not Selected								
AC-17	REMOTE ACCESS	P1 MOD AC-17 (1) (2) (3) (4)	Control: The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	Common Provided by VDC and/or EDUCATE			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-17.1 Examine organizational records or documents to determine if remote access is: (i) monitored on a periodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs. AC-17.2 Examine organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures. AC-17.3 Examine organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials. AC-17.4 Examine the configuration of the information system to determine if controls are employed to restrict remote access to the system. AC-17.5 Examine a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts. AC-17.6 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented. AC-17.7 Test the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions. AC-17.10 Examine organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods. AC-17.11 Examine organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures. AC-17.13 Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions. AC-17.15 Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization controls remote access through a managed access control point.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-17	REMOTE ACCESS	P1 MOD AC-17 (1) (2) (3) (4)	Control Enhancements: (1) The information system monitors and controls remote access methods. (2) The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. (3) The information system routes all remote accesses through [ASSIGNMENT: organization-defined number] managed network access control points (4) The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [ASSIGNMENT: organization-defined needs]; and b. Documents the rationale for such access in the security plan for the information system.	Common Provided by VDC and/or EDUCATE			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			allow privileged access based on compelling operational needs. AC-17.2 Examine organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures. AC-17.3 Examine organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials. AC-17.4 Examine the configuration of the information system to determine if controls are employed to restrict remote access to the system. AC-17.5 Examine a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts. AC-17.6 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented. AC-17.7 Test the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions. AC-17.10 Examine organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods. AC-17.11 Examine organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures. AC-17.13 Interview selected organizational personnel with access control responsibilities and examine the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.	
AC-18	WIRELESS ACCESS	P1 MOD AC-18 (1)	Control: The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections. Control Enhancements: (1) The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	Common Provided by VDC and/or EDUCATE			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-18.1 Examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; (ii) documents, monitors, and controls wireless access to the information system; and (iii) authorizes the use of wireless technologies. AC-18.2 Examine organizational records or documents to determine if the access control policy and procedures are consistent with NIST Special Publication 800-48 and address usage, implementation, monitoring, and authorization of wireless technologies. AC-18.3 Examine organizational records or documents to determine if the organization tracks and monitors wireless access and usage in accordance with organizational policy and procedures. AC-18.4 Examine organizational records or documents to determine if wireless users have been authorized to access the information system. AC-18.5 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the wireless access restrictions control is implemented. Control Enhancements: AC-18(1) Examine the configuration of the information system to determine if wireless access to the system is only permitted through the use of authentication with encryption	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	P1 MOD AC-19 (5)	Control: The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems. Control Enhancements: (1) Not Selected. (2) Not Selected. (3) Not Selected. (4) Not Selected. (5) The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [ASSIGNMENT: organization-defined mobile devices].	Common Provided by VDC and/or EDUCATE			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-19.1 Examine organizational records or documents to determine if: (i) the organization establishes and documents restrictions and implementation guidance for portable and mobile devices; (ii) the organization monitors and controls the use of portable and mobile devices; and (iii) appropriate organizational officials authorize the use of portable and mobile devices and device access to organizational information systems. AC-19.2 Interview selected organizational personnel with access to the information system and examine organizational records or documents detailing the use of portable and mobile devices to determine if personnel are complying with the usage restrictions and applying the implementation guidance on the use of portable and mobile devices in accordance with organization policy and procedures. AC-19.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for portable and mobile devices is implemented. Control Enhancements: AC-19(5) Examine organizational records or documents to determine if the organization employs removable hard drives or cryptography to protect information on portable and mobile devices.	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	P1 MOD AC-20 (1) (2)	Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems. Control Enhancements: (1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. (2) The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AC-20.1 Examine organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of malicious code protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, malicious code definitions, firewall version updates, malicious code protection definitions). AC-20.2 Interview selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting federal information in accordance with access control policy and procedures. AC-20.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owed information systems control is implemented. Control Enhancements: AC-20(1) Examine organizational records or documents to determine if the organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: -can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or -has approved information system connection or processing agreements with the organizational entity hosting the external information system. AC-20(2) Examine organizational records or documents to determine if the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
AC-21	INFORMATION SHARING	P2 MOD AC-21	Control: The Organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [ASSIGNMENT: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [ASSIGNMENT: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.	Hybrid [Note: The quarterly review of accounts covers this. Includes all NFS mounts for systems. Not applicable to VDC.]			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			Examine organizational records or documents to determine if: (i) the organization defines the circumstances where user discretion is required to facilitate information sharing; (ii) the organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the organization-defined circumstances; (iii) the organization defines the information sharing circumstances and automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions; and (iv) the organization employs organization-defined circumstances and automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AC-22	PUBLICLY ACCESSIBLE CONTENT	P2 MOD AC-22	Control: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [ASSIGNMENT: organization-defined frequency] and removes such information, if discovered.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			Examine organizational records or documents to determine if: (i) the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible; (ii) the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; (iii) the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; (iv) the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information; (v) the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization-defined frequency; and (vi) the organization removes nonpublic information from the publicly accessible organizational information system, if discovered.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	P1 MOD AT-1	Control: The organization: a. Develops documents and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose scope roles responsibilities management commitment coordination among organizational entities and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [ASSIGNMENT: organization-defined frequency]; and 2. Security awareness and training procedures [ASSIGNMENT: organization-defined frequency]	Common If additional system/application policy/procedures are in place this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AT-1.1 Examine organizational records or documents to determine if security awareness and training policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated when organizational review indicates updates are required. AT-1.2 Examine the security awareness and training policy to determine if the policy adequately addresses purpose scope roles responsibilities management commitment coordination among organizational entities and compliance. AT-1.3 Examine the security awareness and training procedures to determine if the procedures are sufficient to address all areas identified in the security awareness and training policy and all associated security awareness and training controls. AT-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness and training policy and procedures control is implemented.	
AT-2	SECURITY AWARENESS TRAINING	P1 MOD AT-2(2)	Control: The organization provides basic security awareness training to information system users (including managers senior executives and contractors): a. As part of initial training for new users; b. When required by information system changes; c. [ASSIGNMENT: organization-defined frequency] thereafter. Control Enhancements: (2) The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	Common Hybrid System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AT-2.1 Examine organizational records or documents to determine if: (i) security awareness instruction is provided to all users; (ii) records include the type of instruction received and the date completed; and (iii) initial and refresher instruction is provided in accordance with organization-defined frequency at least annually. AT-2.2 Examine security awareness instructional materials to determine if the materials address the specific requirements of the organization and the information systems to which personnel have authorized access. AT-2.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness control is implemented. Control Enhancements: AT-2(2) Examine organizational records or documents to determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	
AT-3	ROLE-BASED SECURITY TRAINING	P1 MOD AT-3	Control: The organization provides role-based security-related training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [ASSIGNMENT: organization-defined frequency] thereafter.	Common Hybrid System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AT-3.1 Examine organizational records or documents to determine if the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities. AT-3.2 Examine organizational records or documents to determine if: (i) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) the organization provides initial and refresher training in accordance with organization-defined frequency. AT-3.3 Examine the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. AT-3.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training control is implemented.	
AT-4	SECURITY TRAINING RECORDS	P3 MOD AT-4	Control: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [ASSIGNMENT: organization-defined time period].	Common Hybrid System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AT-4.1 Examine organizational records or documents to determine if the organization monitors and fully documents basic security awareness training and specific information system security training. AT-4.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training records control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	P1 MOD AU-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [ASSIGNMENT: organization-defined frequency]; and 2. Audit and accountability procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-1.1 Examine organizational records or documents to determine if audit and accountability policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. AU-1.2 Examine the audit and accountability policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. AU-1.3 Examine the audit and accountability procedures to determine if the procedures are sufficient to address all areas identified in the audit and accountability policy and all associated audit and accountability controls. AU-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit and accountability policy and procedures control is implemented.	
AU-2	AUDIT EVENTS	P1 MOD AU-2 (3)	Control: The organization: a. Determines that the information system is capable of auditing the following events: [ASSIGNMENT: organization-defined list of auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [ASSIGNMENT: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. Control Enhancements: (1) [Withdrawn: Incorporated into AU-12] (2) [Withdrawn: Incorporated into AU-12] (3) The organization reviews and updates the audited events [ASSIGNMENT: organization-defined frequency]. (4) [Withdrawn: Incorporated into AC-6]	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-2.1 Examine organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events. AU-2.2 Test the information system by attempting to perform actions that are configured to generate an audit record. AU-2.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented. Control Enhancements: AU-2(3) Examine organizational records or documents to determine if: (i) the organization defines the frequency of reviews and updates to the list of organization-defined auditable events; and (ii) the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AU-3	CONTENT OF AUDIT RECORDS	P1 MOD AU-3 (1)	Control: : The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Control Enhancements: (1) The information system generates audit records containing the following additional information: [ASSIGNMENT: organization-defined additional, more detailed information].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-3.1 Examine organizational records or documents to determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. AU-3.2 Test the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. AU-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the content of audit records control is implemented. AU-3.6 Examine organizational records or documents to determine if 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. AU-3.7 Test the information system capability to include additional, more detailed information in the audit records for audit events by changing the audit configuration settings to add additional information and by performing actions that create audit records to ensure the additional information is captured. Control Enhancements: AU-3(2).1 Examine organizational records or documents to determine if the organization defines the information system components for which the content of audit records generated is centrally managed.	
AU-4	AUDIT STORAGE CAPACITY	P1 MOD AU-4	Control: The organization allocates audit record storage capacity in accordance with [ASSIGNMENT: organization-defined audit record storage requirements].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-4.1 Examine the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded AU-4.2 Test the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded by artificially generating enough auditable events to create a number of audit records to exceed the storage capacity. AU-4.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit storage capacity control is implemented.	
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	P1 MOD AU-5	Control: The information system: a. Alerts [ASSIGNMENT: organization-defined personnel or roles] in the event of an audit processing failure; and b. 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)].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-5.1 Examine the information system configuration to determine if in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions. AU-5.2 Test the information system configuration to determine in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions by artificially generating auditable events to cause an audit failure or excess capacity condition. AU-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit processing control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	P1 MOD AU-6(1)(3)	Control: The organization: a. Reviews and analyzes information system audit records [ASSIGNMENT: organization-defined frequency] for indications of [ASSIGNMENT: organization-defined inappropriate or unusual activity]; and b. Reports findings to [ASSIGNMENT: organization-defined personnel or roles]. Control Enhancements: (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (2) Not Selected. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-6.1 Examine organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. AU-6.2 Test the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts. AU-6.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented. AU-6.7 Examine organizational records or documents to determine if the organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to enhance the ability to identify inappropriate or unusual activity. Control Enhancements: AU-6(1) Examine organizational records or documents to determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. AU-6(3) Examine organizational records or documents to determine if the organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	
AU-7	AUDIT REDUCTION AND REPORT GENERATION	P2 MOD AU-7 (1)	Control: The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records Control Enhancements: (1) The information system provides the capability to process audit records for events of interest based on [ASSIGNMENT: organization-defined audit fields within audit records].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-7.1 Examine the information system configuration to determine if the system provides an audit reduction and report generation capability. AU-7.2 Test the audit reduction and report generation capability by artificially generating a sufficient number of auditable events to cause an audit reduction and report generation condition. AU-7.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit reduction and report generation control is implemented. Control Enhancements: AU-7(1) Examine organizational records or documents to determine if the organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.	
AU-8	TIME STAMPS	P1 MOD AU-8 (1)	Control: The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [ASSIGNMENT: organization-defined granularity of time measurement]. Control Enhancements: (1) The information system: (a) Compares the internal information system clocks [ASSIGNMENT: organization-defined frequency] with [ASSIGNMENT: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [ASSIGNMENT: organization-defined time period].	Commom Provided by VDC			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-8.1 Examine the information system configuration to determine if the system provides time stamps for use in audit record generation. AU-8.2 Test the use of time stamps within the audit record generation capability of the information system by artificially generating an auditable event at a known time and compare the time stamp on the resulting audit record. AU-8.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the time stamps control is implemented. Control Enhancements: AU-8(1) Examine the configuration settings and test the information system to determine if: (i) the organization defines the frequency of internal clock synchronization for the information system; (ii) the organization defines the authoritative time source for internal clock synchronization; and (iii) the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AU-9	PROTECTION OF AUDIT INFORMATION	P1 MOD AU-9(4)	Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. Control Enhancements: (1) Not Applicable. (2) Not Applicable. (3) Not Applicable. (4) The organization authorizes access to management of audit functionality to only [ASSIGNMENT: organization-defined subset of privileged users].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-9.1 Examine the information system configuration to determine if the system protects audit information and audit tools from unauthorized access, modification, and deletion. AU-9.2 Test the protection of audit information and audit tools from unauthorized access, modification, and deletion by attempting to gain unauthorized access, modify, and delete audit information. AU-9.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the protection of audit information control is implemented.	
AU-10	NON-REPUDIATION	SELECTED FOR HIGH ONLY	Not Selected	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement				
AU-11	AUDIT RECORD RETENTION	P3 MOD AU-11	Control: The organization retains audit records for [ASSIGNMENT: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-11.1 Examine organizational records or documents to determine if the organization retains information system audit logs for an organizationdefined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. AU-11.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit retention control is implemented.	
AU-12	AUDIT GENERATION	P1 MOD AU-12	Control: The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [ASSIGNMENT: organization-defined information system components]; b. Allows [ASSIGNMENT: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 with the content as defined in AU-3.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AU-12.1 Examine organizational records or documents to determine if the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2. AU-12.2 Examine the information system configuration settings to determine if the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2. AU-12.3 Examine the information system configuration settings to determine if the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system. AU-12.4 Test to verify the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	
AU-13	MONITORING FOR INFORMATION DISCLOSURE	NOT SELECTED	Not Selected								
AU-14	SESSION AUDIT	NOT SELECTED	Not Selected								

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	P1 MOD CA-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [ASSIGNMENT: organization-defined frequency]; and 2. Security assessment and authorization procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CA-1.1 Examine organizational records or documents to determine if security assessment, certification, and accreditation policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. CA-1.2 Examine the security assessment, certification, and accreditation policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. CA-1.3 Examine the security assessment, certification, and accreditation procedures to determine if the procedures are sufficient to address all areas identified in the security assessment, certification, and accreditation policy and all associated security assessment, certification, and accreditation controls. CA-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security assessment, certification, and accreditation policies and procedures control is implemented.	
CA-2	SECURITY ASSESSMENTS	P2 MOD CA-2	Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: • Security controls and control enhancements under assessment; • Assessment procedures to be used to determine security control effectiveness; and • Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [ASSIGNMENT: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to to [ASSIGNMENT: organization-defined e. individuals or roles]. Control Enhancement: (1) The organization employs assessors or assessment teams with [ASSIGNMENT: organization-defined level of independence] to conduct security control assessments.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CA-2.1 Examine organizational records or documents to determine if the security controls in the information system are assessed for correct implementation, for intended operation, and for producing the desired outcome with respect to meeting the security requirements for the system in accordance with organization-defined frequency. CA-2.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security assessments control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CA-3	SYSTEM INTERCONNECTIONS	P1 MOD CA-3(5)	Control: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updatesInterconnection Security Agreements [ASSIGNMENT: organization-defined d. frequency]. Control Enhancement: (1) Not Selected. (2) Not Selected. (3) Not Selected. (4) Not Selected. (5) The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [ASSIGNMENT: organization-defined information systems] to connect to external information systems.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CA-3.1 Examine organizational records or documents to determine if all external information systems (i.e., information systems outside of the accreditation boundary that are connected to the information system) are identified and all resulting system connections are authorized and approved by appropriate organizational officials. CA-3.2 Examine information system connection agreements to determine if the agreements are consistent with NIST Special Publication 800-47. CA-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system connections control is implemented. Control Enhancement: CA-3(5) Examine organizational records or documents to determine if the organization employs an allow-all, deny-by-exception or a deny-all, permit-by-exception policy for allowing organization-defined information systems to connect to external information systems.	
CA-5	PLAN OF ACTION AND MILESTONES	P3 MOD CA-5	Control: The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [ASSIGNMENT: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CA-5.1 Examine organizational records or documents to determine if a plan of action and milestones for the information system: (i) exists; (ii) is documented; and (iii) is updated in accordance with organization-defined frequency. CA-5.2 Examine the plan of action and milestones to determine if the plan documents the organization's planned, implemented, and evaluated remedial actions to correct noted deficiencies and to reduce or eliminate known vulnerabilities in the information system. CA-5.3 Examine organizational records or documents to determine if the organization follows the plan of action and milestones (i.e., correcting deficiencies and meeting milestones). CA-5.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the plan of action and milestones control is implemented.	
CA-6	SECURITY AUTHORIZATION	P3 MOD CA-6	Control: The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [ASSIGNMENT: organization-defined frequency].	Common Provided by FSA			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CA-6.1 Examine organizational records or documents to determine if a security accreditation process is defined that authorizes (i.e., accredits) the information system for processing before operations, and updates the authorization within the organization-defined frequency. CA-6.2 Examine organizational records or documents to determine if the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37. CA-6.3 Examine organizational records or documents to determine if a senior organizational official signs and approves the security accreditation. CA-6.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security accreditation control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CA-7	CONTINUOUS MONITORING	P3 MOD CA-7(1)	Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [ASSIGNMENT: organization-defined metrics] to be monitored; b. Establishment of [ASSIGNMENT: organization-defined frequencies] for monitoring and [ASSIGNMENT: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [ASSIGNMENT: organization-defined personnel or roles] [ASSIGNMENT: organization-defined frequency]. Control Enhancement: (1) The organization employs assessors or assessment teams with [ASSIGNMENT: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CA-7.1 Examine organizational records or documents to determine if the organization monitors the security controls in the information system on an ongoing basis. CA-7.2 Examine organizational records or documents to determine if the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A. CA-7.3 Examine organizational records or documents to determine if the organization: (i) assesses designated security controls in the information system; (ii) analyzes for impact, documents, and reports changes to or deficiencies in the operation of the security controls; and (iii) makes adjustments to the information system security plan and plan of action and milestones, as appropriate. CA-7.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the continuous monitoring control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	P1 MOD CM-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [ASSIGNMENT: organization-defined frequency]; and 2. Configuration management procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-1.1 Examine organizational records or documents to determine if the configuration management policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. CM-1.2 Examine the configuration management policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. CM-1.3 Examine the configuration management procedures to determine if the procedures are sufficient to address all areas identified in the configuration management policy and all associated configuration management controls. CM-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration management policies and procedures control is implemented.	
CM-2	BASELINE CONFIGURATION	P1 MOD CM-2 (1) (3) (7)	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancements: (1) The organization reviews and updates the baseline configuration of the information system: (a) [ASSIGNMENT: organization-defined frequency]; (b) When required due to [ASSIGNMENT organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. (2) HIGH Only. (3) The organization retains [ASSIGNMENT: organization-defined previous versions of baseline configurations of the information system] to support rollback. (4) Not Selected. (5) Not Selected. (6) Not Selected. (7) The Organization: a. Issues [ASSIGNMENT: organization-defined information systems, system components, or devices] with [ASSIGNMENT: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and b. Applies [ASSIGNMENT: organization-defined security safeguards] to the devices when the individuals return.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-2.1 Examine organizational records or documents to determine if the organization develops, documents, and maintains a baseline configuration of the information system which includes key architectural components and the relationship among those components. CM-2.2 Examine organizational records or documents to determine if the organization develops, documents, and maintains an inventory of the hardware, software, and firmware components that compose the information system and ownership information by component. CM-2.3 Examine organizational records or documents to determine if the inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture). CM-2.4 Examine organizational records or documents to determine if the inventory of information system components designates those components required to implement and/or conduct contingency operations. CM-2.5 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the baseline configuration and system component inventory control is implemented. CM-2.8 Examine organizational records or documents to determine if the organization identifies: (i) instances that trigger baseline configuration and component inventory updates; (ii) the frequency of updates to the baseline configuration and component inventory; (iii) the dates of baseline configuration and inventory updates, a summary of the updates, and the name of the individuals performing the updates. Control Enhancements: CM-2(1) Examine organizational records or documents to determine if: (i) the organization defines: -the frequency of reviews and updates to the baseline configuration of the information system; and -the circumstances that require reviews and updates to the baseline configuration of the information system; and (ii) the organization reviews and updates the baseline configuration of the information system -in accordance with the organization-defined frequency; -when required due to organization-defined circumstances; and -as an integral part of information system component installations and upgrades. CM-2(3) Examine organizational records or documents to determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback. CM-2(7) Examine organizational records or documents to determine if the organization: (a) Issues organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies organization-defined security safeguards to the devices when the individuals return.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CM-3	CONFIGURATION CHANGE CONTROL	P1 MOD CM-3 (2)	Control: The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [ASSIGNMENT: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [ASSIGNMENT: organization-defined configuration change control element (e.g., committee, board] that convenes [ASSIGNMENT: (one or more): [ASSIGNMENT: organization-defined frequency]; [ASSIGNMENT: organization-defined configuration change conditions]]. Control Enhancements: (1) HIGH Only. (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-3.1 Examine organizational records or documents to determine if the organization documents and controls changes to the information system. CM-3.2 Examine organizational records or documents to determine if appropriate organizational officials approve information system changes in accordance with organizational policy and procedures. CM-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration change control is implemented. Control Enhancements: CM-3(1).2 Test the information system configuration to determine if automated mechanisms are in place to: - document proposed changes to the information system - notify designated approval authorities - highlight approvals that have not been received by the organization-defined time period - inhibit change until designated approvals are received - document completed changes to the information system. CM-3(2) Examine organizational records or documents to determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	
CM-4	SECURITY IMPACT ANALYSIS	P2 MOD CM-4	Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-4.1 Examine organizational records or documents to determine if the organization monitors changes to the information system and identifies the types of changes monitored. CM-4.2 Examine organizational records or documents to determine if the organization performs security impact analyses to assess the effects of changes to the information system. CM-4.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring configuration changes control is implemented.	
CM-5	ACCESS RESTRICTIONS FOR CHANGE	P1 MOD CM-5	Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-5.1 Examine organizational records or documents to determine if the organization maintains a list of personnel authorized to access the information system for purposes of initiating changes, upgrades, and/or modifications to the system. CM-5.2 Examine organizational records or documents to determine if 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. CM-5.3 Examine organizational records or documents identifying changes made to the information system to determine if only authorized personnel initiated, tested, approved, and implemented changes to the system. CM-5.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access restrictions for change control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CM-6	CONFIGURATION SETTINGS	P1 MOD CM-6	Control: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [ASSIGNMENT: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [ASSIGNMENT: organization-defined information system components] based on [ASSIGNMENT: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-6.1 Examine organizational records or documents to determine if 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 operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system. CM-6.2 Examine selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings. CM-6.3 Examine organization documentation or records to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration settings control is implemented.	
CM-7	LEAST FUNCTIONALITY	P1 MOD CM-7 (1)(2)(4)	Control: The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [ASSIGNMENT: organization-defined prohibited or restricted functions, ports, protocols, and/or services]. Control Enhancements: (1) The organization: (a) Reviews the information system [ASSIGNMENT: organization-defined frequency] to identify and unnecessary and/or nonsecure functions, ports, protocols, and/or services; and (b) Disables [ASSIGNMENT: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure]. (2) The information system prevents program execution in accordance with [Selection (one or more): [ASSIGNMENT: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]. (3) Not Selected. (4) The organization: (a) Identifies [ASSIGNMENT: organization-defined software programs not authorized to execute on the information system]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs [ASSIGNMENT: organization defined frequency].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-7.1 Examine organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services. CM-7.2 Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted. CM-7.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least functionality control is implemented. Control Enhancements: CM-7(1) Examine organizational records or documents to determine if the organization defines the frequency of information system reviews to identify and eliminate unnecessary: -functions; -ports; -protocols; and/or -services and the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary: -functions; -ports; -protocols; and/or -services. CM-7(2) Examine organizational records or documents to determine if the organization defines develops and maintains one or more of the following specifications to prevent software program execution on the information system: -a list of software programs authorized to execute on the information system; -a list of software programs not authorized to execute on the information system; and/or -rules authorizing the terms and conditions of software program usage on the information system; and the organization employs automated mechanisms to prevent software program execution on the information system in accordance with the organization-defined specifications.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	P1 MOD CM-8 (1)(3)(5)	Control: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [ASSIGNMENT: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency]. Control Enhancements: (1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. (2) HIGH Only. a. The Organization: a. Employs automated mechanisms [ASSIGNMENT: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and b. Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [ASSIGNMENT: organization-defined personnel or roles]]. b. HIGH Only. (5) The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.	Common If the system relies on operational assets hosted outside VDC, then the control may be hybrid. Also, depending on responsibility for identifying and validating assets at VDC for purpose of inclusion in CMDB, this control may be hybrid.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-8.1 Examine organizational records or documents to determine if the organization defines information deemed necessary to achieve effective property accountability; and the organization develops, documents, and maintains an inventory of information system components that: -accurately reflects the current information system; -is consistent with the authorization boundary of the information system; -is at the level of granularity deemed necessary for tracking and reporting; -includes organization-defined information deemed necessary to achieve effective property accountability; and -is available for review and audit by designated organizational officials. Control Enhancements: CM-8(1) Examine organizational records or documents to determine if the organization updates the inventory of information system components as an integral part of component: -installations; -removals; and -information system updates. CM-8(3).1 Examine organizational records or documents to determine if the organization defines the frequency of employing automated mechanisms to detect the addition of unauthorized components/devices into the information system; CM-8(3).2 Examine organizational records or documents to determine if the organization employs automated mechanisms, in accordance with the organization-defined frequency, to detect the addition of unauthorized components/devices into the information system; and CM-8(3).3 Test the information system configuration to determine if the organization disables network access by such components/devices or notifies designated organizational officials. CM-8(5) Examine organizational records or documents to determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
CM-9	CONFIGURATION MANAGEMENT PLAN	P1 MOD CM-9	Control: The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CM-9 Examine organizational records or documents to determine if the organization develops, documents, and implements a configuration management plan for the information system that: -addresses roles, responsibilities, and configuration management processes and procedures; -defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and -establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	P1 MOD CP-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [ASSIGNMENT: organization-defined frequency]; and 2. Contingency planning procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-1.1 Examine organizational records or documents to determine if contingency planning policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. CP-1.2 Examine the contingency planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. CP-1.3 Examine the contingency planning procedures to determine if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls. CP-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency planning policy and procedures control is implemented.	
CP-2	CONTINGENCY PLAN	P1 MOD CP-2 (1) (3) (8)	2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [ASSIGNMENT: organization-defined personnel or roles]; (2) Distributes copies of the contingency plan to [ASSIGNMENT: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; (3) Coordinates contingency planning activities with incident handling activities; (4) Reviews the contingency plan for the information system [ASSIGNMENT: organization-defined frequency]; (5) Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; (6) Communicates contingency plan changes to [ASSIGNMENT: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and (7) Protects the contingency plan from unauthorized disclosure and modification. Control Enhancements: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans. (2) Not Selected. (3) The organization plans for the resumption of essential missions and business functions within [ASSIGNMENT: organization-defined time period] of contingency plan activation. (4) Not Selected. (5) Not Selcted. (6) Not Selected.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-2.1 Examine organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization. CP-2.2 Examine the contingency plan for the information system to determine if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34. CP-2.3 Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan. CP-2.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented. Control Enhancements: CP-2(1) Examine organizational records or documents to determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans. CP-2(3) Examine organizational records or documents to determine if (i) the organization defines the time period for planning the resumption of essential missions and business functions as a result of contingency plan activation; and (ii) the organization plans for the resumption of essential missions and business function within organization-defined time period of contingency plan activation. CP-2(8) Examine organizational records or documents to determine if the organization identifies critical information system assets supporting essential missions and business functions.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CP-3	CONTINGENCY TRAINING	P2 MOD CP-3	Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [ASSIGNMENT: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [ASSIGNMENT: organization-defined frequency] thereafter.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-3.1 Examine organizational records or documents to determine if the organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities. CP-3.2 Examine organizational records or documents to determine if the organization: (i) provides contingency training to personnel with significant contingency roles and responsibilities or personnel implementing the contingency plan; (ii) records the type of contingency training received and the date completed; and (iii) provides initial and refresher training in accordance with organization-defined frequency, at least annually. CP-3.3 Examine the contingency training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. CP-3.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency training control is implemented.	
CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	P2 MOD CP-4 (1)	Control: The organization: a. Tests the contingency plan for the information system [ASSIGNMENT: organization-defined frequency] using [ASSIGNMENT: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed. Control Enhancements: (1) The organization coordinates contingency plan testing with organizational elements responsible for related plans.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-4.1 Examine organizational records or documents to determine if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests. CP-4.2 Examine organizational records or documents to determine if the organization reviews the contingency plan test results and takes corrective actions. CP-4.3 Examine organizational records or documents to determine if the contingency plan tests or exercises address key aspects of the plan and if the tests or exercises confirm that the plan objectives are met. CP-4.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan testing control is implemented. CP-4.8 Examine organizational records or documents to determine if 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). Control Enhancements: CP-4(1) Examine organizational records or documents to determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	
CP-6	ALTERNATE STORAGE SITE	P1 MOD CP-6 (1) (3)	Control: The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site. Control Enhancements: (1) The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same hazards. (2) HIGH Only. (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.	Common If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-6.1 Examine organizational records or documents to determine if alternate storage site agreements are currently in place to permit storage of information system backup information. CP-6.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate storage site control is implemented. Control Enhancements: CP-6(1).1 Examine the contingency plan to determine if the plan identifies the primary storage site hazards. CP-6(3) Examine organizational records or documents to determine if: (i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CP-7	ALTERNATE PROCESSING SITE	P1 MOD CP-7 (1) (2) (3)	Control: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [ASSIGNMENT: organization-defined information system operations] for essential missions/business functions within [ASSIGNMENT: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site. Control Enhancements: (1) The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. (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) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).	Common If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-7.1 Examine organizational records or documents to determine if alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period. CP-7.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate processing site control is implemented. Control Enhancements: CP-7(1).1 Examine the contingency plan to determine if the plan identifies the primary processing site hazards. CP-7(1).2 Examine the alternate processing site to determine if the site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site. CP-7(2) Examine the contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems. CP-7(3) Examine alternate processing site agreements to determine if the agreements contain priority of service provisions in accordance with the organization's availability requirements.	
CP-8	TELECOMMUNICATIONS SERVICES	P1 MOD CP-8 (1) (2)	Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [ASSIGNMENT: organization-defined information system operations] for essential missions and business functions within [ASSIGNMENT: organization defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. Control Enhancements: (1) The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. (2) The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-8.1 Examine alternate telecommunication service agreements to determine if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable. CP-8.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the telecommunications services control is implemented. Control Enhancements: CP-8(1) Examine primary and alternate telecommunication service agreements to determine if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan. CP-8(2) Examine primary and alternate telecommunications service agreements and interview appropriate telecommunications service providers to determine if alternate and primary telecommunications services share a single point of failure.	
CP-9	INFORMATION SYSTEM BACKUP	P1 MOD CP-9 (1)	Control: The organization: a. Conducts backups of user-level information contained in the information system [ASSIGNMENT: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [ASSIGNMENT: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups ofinformation system documentation including security-related documentation [ASSIGNMENT: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations. Control Enhancements: (1) The organization tests backup information [ASSIGNMENT: organization-defined frequency] to verify media reliability and information integrity.	Common If system operations rely on assets that are not backed up by VDC or EDUCATE, or the system performs additional backups, this control may be hybrid.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-9.1 Examine organizational records or documents to determine if the organization defines the user-level and system-level information (including system state information) that is required to be backed up and identifies the location for storing backup information. CP-9.2 Examine selected information system backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures. CP-9.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup control is implemented. Control Enhancements: CP-9(1) Examine organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	P1 MOD CP-10 (2)	Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Control Enhancements: (1) [Withdrawn: Incorporated into CP-4]. (2) The information system implements transaction recovery for systems that are transaction-based. (3) [Withdrawn: Addressed through tailoring procedures.]	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			CP-10.1 Examine organizational records or documents to determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system. CP-10.2 Examine organizational records or documents to determine if the organization identifies means for capturing the information system's operational state including all system parameters, patches, configuration settings, and application/system software prior to system disruption or failure. CP-10.3 Examine organizational records or documents to determine if the organization tests the information system after completion of recovery and reconstitution operations. CP-10.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system recovery and reconstitution control is implemented. Control Enhancements: CP-10(2) Examine organizational records or documents to determine if the information system implements transaction recovery for systems that are transaction-based.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	P1 MOD IA-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [ASSIGNMENT: organization-defined frequency];and 2. Identification and authentication procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IA-1.1 Examine organizational records or documents to determine if identification and authentication policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. IA-1.2 Examine the identification and authentication policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. IA-1.3 Examine the identification and authentication procedures to determine if the procedures are sufficient to address all areas identified in the identification and authentication policy and all associated identification and authentication controls. IA-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identification and authentication policy and procedures control is implemented.	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	P1 MOD IA-2 (1) (2) (3) (8) (11)(12	Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system implements multifactor authentication for network access to privileged accounts (2) The information system implements multifactor authentication for network access to nonprivileged accounts. (3) The information system implements multifactor authentication for local access to privileged accounts. (4) HIGH Only. (5) Not Selected. (6) Not Selected. (7) Not Selected. (8) The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. (9) Not Selected. (10) Not Slected. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [ASSIGNMENT: organization-defined strength of mechanism requirements]. (12) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials	Common, Hybrid IF SYSTEM USES AIMS, COMMON ELSE HYBRID (system specifc for app accounts, but VDC provided for "backend" accounts)			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			with NIST Special Publication 800-63. IA-2.3 Test the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST Special Publication 800-63. IA-2.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user identification and authentication control is implemented. Control Enhancements: IA-2(1) Examine the configuration settings and test the information system to determine if the information system uses multifactor authentication for network access to privileged accounts. IA-2(2) Examine the configuration settings and test the information system to determine if the information system uses multifactor authentication for network access to non-privileged accounts. IA-2(3) Examine the configuration settings and test the information system to determine if the information system uses multifactor authentication for local access to privileged accounts. IA-2(8) Examine the configuration settings and test the information system to determine if: (i) the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and (ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts. IA-2(11) Examine the configuration settings and test the information system to determine if the information system implements multifactor	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	P1 MOD IA-3	Control: The information system uniquely identifies and authenticates [ASSIGNMENT: organization-defined specific and/ or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Common (Hybrid / System-Specific) NOTE:DEPENDS ON SETUP. Likely Common if no system-to-system interfaces			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IA-3.1 Examine organizational records or documents and information system configuration settings to determine if 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-3.2 Examine organizational records or documents to determine if the strength of the device authentication mechanism is consistent with the FIPS 199 security categorization of the information system. IA-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the device authentication and authentication control is implemented.	
IA-4	IDENTIFIER MANAGEMENT	P1 MOD IA-4	Control: The organization manages information system identifiers by: a. Receiving authorization from [ASSIGNMENT: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiersfor [ASSIGNMENT: organization-defined time period]; and e. Disabling the identifier after [ASSIGNMENT: organization-defined time period of inactivity].t	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IA-4.1 Examine organizational records or documents and information system configuration settings to determine if 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 an organization-defined time period of inactivity; and (vi) archiving user identifiers. IA-4.2 Examine organizational records or documents to determine if a personal identity verification (PIV) card token is used 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. IA-4.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identifier management control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IA-5	AUTHENTICATOR MANAGEMENT	P1 MOD IA-5 (1) (2) (3) (11)	Control: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [ASSIGNMENT: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring individuals to take, and having devices implement, specific security safeguards protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes. Control Enhancements: (1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [ASSIGNMENT: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (b) Enforces at least the following number of changed characters when new passwords are created: [ASSIGNMENT: organization-defined number]; (c) Stores and transmits only encrypted representations of passwords; (d) Enforces password minimum and maximum lifetime restrictions of [ASSIGNMENT: organization defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [ASSIGNMENT: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password. (2) The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network. (3) The organization requires that the registration process to receive [ASSIGNMENT: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [ASSIGNMENT: organization-defined registration authority] with authorization by [ASSIGNMENT: organization-defined personnel or roles].). (4) Not Selected. (5) Not Selected. (6) Not Selected. (7) Not Selected. (8) Not Selected. (9) Not Selected. (10) Not Selected. (11) The information system, for hardware token-	Common, Hybrid IF SYSTEM USES AIMS, COMMON IF SYSTEM USES PIN, MAY ALSO BE COMMON (if PIN outside of boundaries) ELSE HYBRID (system specifc for app accounts, but VDC provided for "backend" accounts)			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement		IA-5.1 Examine organizational records or documents and the information system configuration settings to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations. IA-5.2 Examine organizational records or documents to determine if the organization establishes administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. IA-5.3 Examine organizational records or documents to determine if the organization changes default authenticators upon information system installation. IA-5.4 Interview selected organizational personnel with identification and authentication responsibilities to determine if 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. IA-5.5 Examine organizational records or documents to determine if the information system establishes user control of the corresponding private key and maps the authenticated identity to the user account (for PKI-based authentication). IA-5.6 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator management control is implemented. Control Enhancements: IA-5(1) Examine the configuration settings and test the information system to determine if: (i) the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type; (ii) the organization defines the minimum number of characters that must be changed when new passwords are created; (iii) the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters; (iv) the organization defines the number of generations for which password reuse is prohibited; and (v) the information system, for password-based authentication: -enforces the minimum password complexity standards that meet the organization-defined requirements; -enforces the organization-defined minimum number of characters that must be changed when new passwords are created; -encrypts passwords in storage and in transmission; -enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and -prohibits password reuse for the organization-defined number of generations. IA-5(2) Examine the configuration settings and test the information system to determine if the information system, for PKI-based authentication: -validates certificates by constructing a certification path with status information to an accepted trust anchor; -enforces authorized access to the corresponding private key; and -maps the authenticated identity to the user account. IA-5(3) Examine organizational records or documents to determine if: (i) the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and (ii) the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). IA-5(11) Examine the configuration settings and test the information system to determine if the information system, for hardware token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	Template Date March 6, 2014

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IA-6	AUTHENTICATOR FEEDBACK	P1 MOD IA-6	Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Common, Hybrid IF SYSTEM USES AIMS, COMMON IF SYSTEM USES PIN, MAY ALSO BE COMMON (if PIN outside of boundaries) ELSE HYBRID (system specifc for app accounts, but VDC provided for "backend" accounts)			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IA-6.1 Examine organizational records or documents and information system configuration settings to determine if the system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). IA-6.2 Test the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism. IA-6.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator feedback control is implemented.	
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	P1 MOD IA-7	Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Common Provided by VDC			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IA-7.1 Examine organizational records or documents and information system configuration settings to determine if the system employs authentication methods for authentication to a cryptographic module that meet the requirements of FIPS 140-2. IA-7.2 Examine organizational records or documents and information system configuration settings to determine if the information system employs authentication methods 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. IA-7.3 Examine organizational records or documents to determine if the organization clearly documents authentication methods to a cryptographic module for the information system. IA-7.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic module authentication control is implemented.	
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	P1 MOD IA-8(1)(2)(3)(4)	Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Control Enhancement: (1) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. (2) The information system accepts only FICAM-approved third-party credentials (3) The organization employs only FICAM-approved information system components in [ASSIGNMENT: organization-defined information systems] to accept third-party credentials. (4) The information system conforms to FICAM-issued profiles.	Common, Hybrid IF SYSTEM USES AIMS, COMMON IF SYSTEM USES PIN, MAY ALSO BE COMMON (if PIN outside of boundaries) ELSE HYBRID (system specifc for app accounts, but VDC provided for "backend" accounts)			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IA-8 Examine organizational records or documents to determine if the organization defines the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Control Enhancement: IA-8(1) Examine the information system documentation or configuration settings to determine if the information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. IA-8(2) Examine the information system documentation or configuration settings to determine if the information system accepts only Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. IA-8(3) Examine organizational records or documents to determine if the organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials. IA-8(4) Examine the information system documentation or configuration settings to determine if the information system conforms to FICAM-issued profiles.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	P1 MOD IR-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [ASSIGNMENT: organization-defined frequency]; and 2. Incident response procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-1.1 Examine organizational records or documents to determine if incident response policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. IR-1.2 Examine the incident response policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. IR-1.3 Examine the incident response procedures to determine if the procedures are sufficient to address all areas identified in the incident response policy and all associated incident response controls. IR-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response policy and procedures control is implemented.	
IR-2	INCIDENT RESPONSE TRAINING	P2 MOD IR-2	Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [ASSIGNMENT: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [ASSIGNMENT: organization-defined frequency] thereafter.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-2.1 Examine organizational records or documents to determine if the organization identifies personnel with significant incident response roles and responsibilities and documents those roles and responsibilities. IR-2.2 Examine organizational records or documents to determine if: (i) incident response training is provided to personnel with significant incident response roles and responsibilities; (ii) records include the type of incident response training received and the date completed; and (iii) initial and refresher training is provided in accordance with organization-defined frequency, at least annually. IR-2.3 Examine the incident response training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. IR-2.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response training control is implemented.	
IR-3	INCIDENT RESPONSE TESTING	P2 MOD IR-3 (2)	Control: The organization tests the incident response capability for the information system [ASSIGNMENT: organization-defined frequency] using [ASSIGNMENT: organization-defined tests] to determine the incident response effectiveness and documents the results. Control Enhancements: (1) Not Selected. (2) The organization coordinates incident response testing with organizational elements responsible for related plans.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-3.1 Examine organizational records or documents to determine if the organization tests its incident response capability using the organization defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests. IR-3.2 Examine organizational records or documents to determine if the organization reviews incident response test results and takes corrective actions. IR-3.3 Examine organizational records or documents to determine if the incident response tests or exercises address key aspects of the incident response capability and if the tests or exercises confirm that the incident response objectives are met. IR-3.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response testing control is implemented. Control Enhancements: IR-3(2) Examine organizational records or documents to determine if the organization coordinates incident response testing with organizational elements responsible for related plans.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IR-4	INCIDENT HANDLING	P1 MOD IR-4 (1)	Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Control Enhancements: (1) The organization employs automated mechanisms to support the incident handling process.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-4.1 Examine organizational records or documents to determine if the organization implements an incident handling capability for the information system that includes preparation, detection and analysis, containment, eradication, and recovery. IR-4.2 Examine organizational records or documents (or personnel engaged in incident handling activities) to determine if personnel are following designated incident handling procedures. IR-4.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident handling control is implemented. Control Enhancements: IR-4(1)Examine organizational records or documents to determine if incident handling functions are automated.	
IR-5	INCIDENT MONITORING	P1 MOD IR-5	Control: The organization tracks and documents information system security incidents.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-5.1 Examine organizational records or documents to determine if the organization tracks and documents information system security incidents on an ongoing basis. IR-5.2 Examine organizational records or documents (or personnel engaged in incident monitoring activities) to determine if personnel are following designated incident monitoring procedures. IR-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident monitoring control is implemented.	
IR-6	INCIDENT REPORTING	P1 MOD IR-6(1)	Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [ASSIGNMENT: organization-defined time-period]; and b. Reports security incident information to [ASSIGNMENT: organization-defined authorities]. Control Enhancements: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-6.1 Examine organizational records or documents to determine if theorganization promptly reports incident information to appropriate authorities. IR-6.2 Examine organizational records or documents (or personnel engaged in incident reporting activities) to determine if personnel are following designated incident reporting procedures. IR-6.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident reporting control is implemented. Control Enhancements: IR-6(1) Examine organizational records or documents to determine if incident reporting functions are automated.	
IR-7	INCIDENT RESPONSE ASSISTANCE	P3 MOD IR-7 (1)	Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Control Enhancements: (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	Common Provided by VDC			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-7.1 Examine organizational records or documents to determine if the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. IR-7.2 Examine organizational records or documents (or personnel engaged in incident response support activities) to determine if personnel are following designated incident response support procedures. IR-7.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response assistance control is implemented. Control Enhancements: IR-7(1) Examine organizational records or documents to determine if incident response support functions are automated.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
IR-8	INCIDENT RESPONSE PLAN	P1 MOD IR-8	Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization. 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [ASSIGNMENT: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [ASSIGNMENT: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [ASSIGNMENT: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [ASSIGNMENT: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]. f. Protects the incident response plan from unauthorized disclosure and modification.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			IR-8.1 Examine organizational records or documents to determine if the organization develops an incident response plan that: -provides the organization with a roadmap for implementing its incident response capability; -describes the structure and organization of the incident response capability; -provides a high-level approach for how the incident response capability fits into the overall organization; -meets the unique requirements of the organization, which relate to mission, size, structure, and functions; -defines reportable incidents; -provides metrics for measuring the incident response capability within the organization; -defines the resources and management support needed to effectively maintain and mature an incident response capability; and -is reviewed and approved by designated officials within the organization. IR-8.2 Examine organizational records or documents to determine if: (i) the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements; (ii) the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan; (iii) the organization defines, in the incident response plan, the frequency to review the plan; (iv) the organization reviews the incident response plan in accordance with the organization-defined frequency; (v) the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and (vi) the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	P1 MOD MA-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [ASSIGNMENT: organization-defined frequency]; and 2. System maintenance procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MA-1.1 Examine organizational records or documents to determine if the information system maintenance policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. MA-1.2 Examine the information system maintenance policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. MA-1.3 Examine the information system maintenance procedures to determine if the procedures are sufficient to address all areas identified in the information system maintenance policy and all associated information system maintenance controls. MA-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system maintenance policy and procedures control is implemented.	
MA-2	CONTROLLED MAINTENANCE	P2 MOD MA-2	Control: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [ASSIGNMENT: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [ASSIGNMENT: organization-defined maintenance-related information] in organizational maintenance records.	Common, Hybrid WHILE FSA GENERALLY THINKS OF THESE CONTROLS AS COMMON, WE MUST NOTE THAT, TO THE EXTENT THAT AN APPLICATION-SUPPORT TEAM MUST CONDUCT INTEGRATION TESTING UPON INFRASTRUCTURE MAINTENANCE, AND MAY, UNDER CERTAIN CIRCUMSTANCES, MODIFY THE APPLICATION DUE TO INFRASTRUCTURE CHANGES, THIS CONTROL COULD BE DEEMED			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MA-2.1 Examine organizational records or documents to determine if the organization schedules and performs routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. MA-2.2 Examine organizational records or documents to determine if the organization fully documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational periodic maintenance requirements. MA-2.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the periodic maintenance control is implemented. MA-2.6 Examine the maintenance log to determine if the log 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).	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
MA-3	MAINTENANCE TOOLS	P2 MOD MA-3 (1) (2)	Control Enhancements: (1) The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. (2) The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system. (3) HIGH Only.	Common, Hybrid NOTE: WHILE FSA GENERALLY THINKS OF THESE CONTROLS AS COMMON, WE MUST NOTE THAT, TO THE EXTENT THAT AN APPLICATION-SUPPORT TEAM FOR A COTS PRODUCT, FOR EXAMPLE, MUST OBTAIN MAINTENANCE SUPPORT FOR THE APPLICATION, THIS MAY BE A "HYBRID" CONTROL			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MA-3.1 Examine organizational records or documents to determine if the organization approves, controls, and monitors information system maintenance tools. MA-3.2 Examine approved information system maintenance tools and associated documentation to determine if the organization maintains the tools and documentation on an ongoing basis and if the processes applied are consistent with the documented maintenance procedures. MA-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance tools control is implemented. Control Enhancements: MA-3(1) Examine organizational records or documents to determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. MA-3(2) Examine organizational records or documents to determine if the organization checks all media containing diagnostic and test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.	
MA-4	NONLOCAL MAINTENANCE	P1 MOD MA-4 (2)	Control: The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed. Control Enhancements: (1) Not Selected. (2) The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	Common, Hybrid WHILE FSA GENERALLY THINKS OF THESE CONTROLS AS COMMON, WE MUST NOTE THAT, TO THE EXTENT THAT AN APPLICATION-SUPPORT TEAM FOR A COTS PRODUCT, FOR EXAMPLE, MUST OBTAIN MAINTENANCE SUPPORT FOR THE APPLICATION, THIS MAY BE A "HYBRID" CONTROL			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MA-4.1 Examine organizational records or documents to determine if the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities. MA-4.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote maintenance control is implemented. Control Enhancements: MA-4(2) Examine organizational records or documents to determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system.	
MA-5	MAINTENANCE PERSONNEL	P1 MOD MA-5	Control: The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Common, Hybrid WHILE FSA GENERALLY THINKS OF THESE CONTROLS AS COMMON, WE MUST NOTE THAT, TO THE EXTENT THAT AN APPLICATION-SUPPORT TEAM FOR A COTS PRODUCT, FOR EXAMPLE, MUST OBTAIN MAINTENANCE SUPPORT FOR THE APPLICATION, THIS MAY BE A "HYBRID" CONTROL			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MA-5.1 Examine organizational records or documents to determine if: (i) the organization maintains a list of personnel authorized to perform maintenance on the information system; and (ii) only authorized personnel have performed maintenance on the information system. MA-5.2 Examine organizational records or documents to determine if theorganization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance personnel control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
MA-6	TIMELY MAINTENANCE	P1 MOD MA-6	Control: The organization obtains maintenance support and/or spare parts for [ASSIGNMENT: organization-defined information system components] within [ASSIGNMENT: organization-defined time period] of failure.	Common, Hybrid WHILE FSA GENERALLY THINKS OF THESE CONTROLS AS COMMON, WE MUST NOTE THAT, TO THE EXTENT THAT AN APPLICATION-SUPPORT TEAM FOR A COTS PRODUCT, FOR EXAMPLE, MUST OBTAIN MAINTENANCE SUPPORT FOR THE APPLICATION, THIS MAY BE A "HYBRID" CONTROL			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MA-6.1 Examine organizational records or documents to determine if maintenance support agreements and the inventory of spare parts are sufficient to support the organization-defined list of key information system components within the organization-defined time period of failure. MA-6.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the timely maintenance control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	P1 MOD MP-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [ASSIGNMENT: organization-defined frequency]; and 2. Media protection procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MP-1.1 Examine organizational records or documents to determine if the media protection policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated when organizational reviews indicate updates are required. MP-1.2 Examine the media protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. MP-1.3 Examine the media protection procedures to determine if the procedures are sufficient to address all areas identified in the media protection policy and all associated media protection controls. MP-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media protection policy and procedures control is implemented.	
MP-2	MEDIA ACCESS	P1 MOD MP-2	Control: The organization restricts access to [ASSIGNMENT: organization-defined types of digital and/ or non-digital media] to [ASSIGNMENT: organization-defined personnel or roles].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MP-2.1 Examine organizational records or documents and/or physical facilities containing media devices to determine if only authorized users have access to information in printed form or on digital media removed from the information system. MP-2.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media access control is implemented.	
MP-3	MEDIA MARKING	P1 MOD MP-3	Control: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [ASSIGNMENT: organization-defined types of information system media] from marking as long as the media remain within [ASSIGNMENT: organization-defined controlled areas].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MP-3 Examine organizational records or documents to determine if: (i) the organization defines removable media types and information system output that require marking; (ii) the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; (iii) the organization defines: -removable media types and information system output exempt from marking; -controlled areas designated for retaining removable media and information output exempt from marking; and (iv) removable media and information system output exempt from marking remain within designated controlled areas.	
MP-4	MEDIA STORAGE	P1 MOD MP-4	Control: The organization: a. Physically controls and securely stores [ASSIGNMENT: organization-defined types of digital and/ or non-digital media] within [ASSIGNMENT: organization-defined controlled areas]. b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MP-4.1 Examine organizational records or documents to determine if the organization protects information system media at the highest FIPS 199 security category for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures. MP-4.2 Examine the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media. MP-4.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media storage control is implemented.	
MP-5	MEDIA TRANSPORT	P1 MOD MP-5(4)	Control: The organization: a. Protects and controls [ASSIGNMENT: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [ASSIGNMENT: organization-defined security safeguards]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel. Control Enhancements: (1) [Withdrawn: Incorporated into MP-5]. (2) [Withdrawn: Incorporated into MP-5]. (3) Not Selected. (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MP-5.1 Examine organizational records or documents to determine if the organization restricts the pickup, receipt, transfer, and delivery of information system media (paper and digital) to authorized personnel. MP-5.2 Examine the list of personnel that have been authorized for the pickup, receipt, transfer, and delivery of information system media to determine if access is appropriately restricted. MP-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media transport control is implemented. Control Enhancements: MP-5(4) Examine organizational records or documents to determine if the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
MP-6	MEDIA SANITIZATION	P1 MOD MP-6	Control: The organization: a. Sanitizes [ASSIGNMENT: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [ASSIGNMENT: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			MP-6.1 Examine organizational records or documents to determine if the organization: (i) sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii)conducts periodic tests of sanitization equipment to ensure correct performance. MP-6.2 Examine organizational records or documents to determine if the organization sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse consistent with NIST Special Publication 800-88. MP-6.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media sanitization and disposal control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	P1 MOD PE-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [ASSIGNMENT: organization-defined frequency]; and 2. Physical and environmental protection procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-1.1 Examine organizational records or documents to determine if the physical and environmental protection policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. PE-1.2 Examine the physical and environmental protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. PE-1.3 Examine the physical and environmental protection procedures to determine if the procedures are sufficient to address all areas identified in the physical and environmental protection policy and all associated physical and environmental protection controls. PE-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical and environmental protection policy and procedures control is implemented.	
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	P1 MOD PE-2	Control: The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [ASSIGNMENT: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-2.1 Examine organizational records or documents to determine if: (i) the organization develops and keeps current a list of personnel with authorized access to the facility containing the information system; (ii) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (iii) designated officials within the organization review and approve the access list and authorization credentials on an organization-defined frequency. PE-2.2 Examine the facility access list to determine if: (i) the individuals on the list are current personnel assigned to the organization; and (ii) the authorization credentials of the personnel are appropriate. PE-2.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access authorizations control is implemented.	
PE-3	PHYSICAL ACCESS CONTROL	P1 MOD PE-3	Control: The organization: a. Enforces physical access authorizations at [ASSIGNMENT: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [ASSIGNMENT: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [ASSIGNMENT: organization-defined entry/exit points]; c. Provides [ASSIGNMENT: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [ASSIGNMENT: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [ASSIGNMENT: organization-defined physical access devices] every [ASSIGNMENT: organization-defined frequency]; and g. Changes combinations and keys [ASSIGNMENT: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-3.1 Examine organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. PE-3.2 Examine organizational records or documents and selected physical access devices to determine if; (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated. PE-3.3 Examine organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST Special Publication 800-76 (where the token-based access control function employs biometric verification). PE-3.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	P1 MOD PE-4	Control: The organization controls physical access to [ASSIGNMENT: organization-defined information system distribution and transmission lines] within organizational facilities using [ASSIGNMENT: organization-defined security safeguards].	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-4.1 Examine organizational records or documents to determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.	
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	P1 MOD PE-5	Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-5.1 Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output. PE-5.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for display medium control is implemented.	
PE-6	MONITORING PHYSICAL ACCESS	P1 MOD PE-6 (1)	Control: The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [ASSIGNMENT: organization-defined frequency] and upon occurrence of [ASSIGNMENT: organization-defined events or potential indications of events]; and c. c. Coordinates results of reviews and investigations with the organizational incident response capability. Control Enhancements: (1) The organization monitors physical intrusion alarms and surveillance equipment.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-6.1 Examine organizational records, documents, and the facility where the information system resides to determine if the organization monitors physical access to information systems to detect and respond to incidents. PE-6.2 Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine how individuals respond to physical access incidents. PE-6.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring physical access control is implemented. Control Enhancements: PE-6(1) Examine intrusion alarms and surveillance equipment to determine if the organization monitors real-time physical intrusion alarms and surveillance equipment.	
PE-8	VISITOR ACCESS RECORDS	P3 MOD PE-8	Control: The organization: a. Maintains visitor access records to the facility where the information system resides for [ASSIGNMENT: organization-defined time period]; and b. Reviews visitor access records [ASSIGNMENT: organization-defined frequency].	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-8.1 Examine organizational records or documents to determine if the organization maintains a visitor access log to the facility where the information system resides 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; (vii) name and organization of person visited; and (viii) an indication of a designated official's review of the access log within the organization defined frequency. PE-8.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access logs control is implemented.	
PE-9	POWER EQUIPMENT AND CABLING	P1 MOD PE-9	Control: The organization protects power equipment and power cabling for the information system from damage and destruction.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-9.1 Examine organizational records, documents, and the facility where the information system resides to determine if the organization protects power equipment and power cabling for the information system from damage and destruction. PE-9.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the power equipment and power cabling control is implemented.	
PE-10	EMERGENCY SHUTOFF	P1 MOD PE-10	Control: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [ASSIGNMENT: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-10.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization provides the capability of shutting off power to any information system component that may be malfunctioning or threatened. PE-10.2 Examine the emergency shutoff capability to ensure that it exists and is functional. PE-10.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency shutoff control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PE-11	EMERGENCY POWER	P1 MOD PE-11	Control: The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-11.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss. PE-11.2 Examine organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a shortterm power supply for the information system. PE-11.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency power control is implemented. Control Enhancements: PE-11(1) Examine the physical site location to determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	
PE-12	EMERGENCY LIGHTING	P1 MOD PE-12	Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-12.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains an automatic emergency lighting system that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes. PE-12.2 Examine organizational records or documents to determine if the results of the last tested power outage demonstrated that the emergency lighting system was operational and fully functional. PE-12.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency lighting control is implemented.	
PE-13	FIRE PROTECTION	P1 MOD PE-13(3)	Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-13.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. PE-13.2 Examine the results of the last test of the fire suppression and detection devices/systems to determine if the fire protection resources can be successfully activated in the event of a fire. PE-13.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the fire protection control is implemented. PE-13.6 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if fire suppression and detection devices/systems activate automatically in the event of a fire. Control Enhancements: PE-13(3) Examine the information system documentation or configuration settings to determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	P1 MOD PE-14	Control: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [ASSIGNMENT: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [ASSIGNMENT: organization-defined frequency].	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-14.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization regularly maintains, within acceptable levels, and monitors the temperature and humidity of the facility where the information system resides. PE-14.2 Examine the facility where the information system resides to determine if the temperature and humidity controlling systems are in place and functioning as intended. PE-14.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the temperature and humidity control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PE-15	WATER DAMAGE PROTECTION	P1 MOD PE-15	Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-15.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization protects the information system from water damage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. PE-15.2 Examine the facility where the information system resides to determine if the master shutoff valves are accessible and working properly. PE-15.3 Examine organizational records or documents to determine if the results of the last test of the environmental controls of the facility where the information system resides demonstrate that the master shutoff valves are working properly. PE-15.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the water damage protection control is implemented.	
PE-16	DELIVERY AND REMOVAL	P2 MOD PE-16	Control: The organization authorizes, monitors, and controls [ASSIGNMENT: organization-defined types of information system components] entering and exiting the facility and maintains records of those items..	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-16.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization controls the information system-related items (i.e., hardware, firmware, software) entering and exiting the facility where the system resides and maintains appropriate records of those items. PE-16.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the delivery and removal control is implemented.	
PE-17	ALTERNATE WORK SITE	P2 MOD PE-17	Control: The organization: a. Employs [ASSIGNMENT: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Common, Hybrid THIS CONTROL IS MOST LIKELY HYBRID COMMON CONTROL MAY BE PROVIDED BY VDC OR EDUCATE (such as for support teams located at UCP)			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-17.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if individuals within the organization employ appropriate information system security controls at alternate work sites. PE-17.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate work site control is implemented.	
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	SELECTED FOR HIGH ONLY	Not Selected	Common, Hybrid If the system relies on operational assets hosted outside VDC, then the control may be hybrid			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PE-18.1 Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization positions information system components within the facility to minimize potential damage from environmental hazards (e.g., electrical interference, electromagnetic radiation, vandalism, eating, drinking, smoking in the proximity, information leakage due to emanation) and to minimize the opportunity for unauthorized access. PE-18.2 Examine the facility where the information system components reside to determine if the organization positions components to minimize potential damage from environmental hazards and to minimize the opportunity for unauthorized access. PE-18.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the location of information system components control is implemented.	
PE-19	INFORMATION LEAKAGE	NOT SELECTED	Not Selected								

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	P1 MOD PL-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [ASSIGNMENT: organization-defined frequency]; and 2. Security planning procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PL-1.1 Examine organizational records or documents to determine if security planning policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. PL-1.2 Examine the security planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. PL-1.3 Examine the security planning procedures to determine if the procedures are sufficient to address all areas identified in the security planning policy and all associated security planning controls. PL-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security planning policy and procedures control is implemented.	
PL-2	SYSTEM SECURITY PLAN	P1 MOD PL-2(3)	Control: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [ASSIGNMENT: organization-defined personnel or roles]; c. Reviews the security plan for the information system [ASSIGNMENT: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification. Control Enhancements: (1) Incorporated into PL-7 (2) Incorportaed into PL-8 (3) The organization plans and coordinates security-related activities affecting the information system with [ASSIGNMENT: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PL-2.1 Examine organizational records or documents to determine if the security plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization. PL-2.2 Examine the security plan to determine if the plan is consistent with NIST Special Publication 800-18 and addresses security roles, responsibilities, assigned individuals with contact information, and activities for planning security of the information system. PL-2.3 Interview selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the security plan and are ready to implement the plan. PL-2.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system security plan control is implemented. Control Enhancements: PL-2(3) Examine organizational records or documents to determine if the organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PL-4	RULES OF BEHAVIOR	P2 MOD PL-4(1)	Control: The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. Control Enhancement: (1) The organization includes in the rules of behavior, explicit restrictions on the use of social media/ networking sites and posting organizational information on public websites.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PL-4.1 Examine organizational records or documents to determine if the organization provides and makes readily available to all information system users a set of rules that describes users responsibilities and expected behavior with regard to information and information system usage. PL-4.2 Examine organizational records or documents to determine if the organization receives a 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. PL-4.3 Examine the rules of behavior to determine if the content is consistent with NIST Special Publication 800-18. PL-4.4 Interview selected organizational personnel to determine if they understand the rules of behavior for the information system. PL-4.5 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the rules of behavior control is implemented. Control Enhancements: PL-4(1) Examine organizational records or documents to determine if the organization includes in the rules of behavior: -explicit restrictions on the use of social networking sites; -posting information on commercial Web sites; and -sharing information system account information.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	P1 MOD PS-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [ASSIGNMENT: organization-defined frequency]; and 2. Personnel security procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-1.1 Examine organizational records or documents to determine if the personnel security policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. PS-1.2 Examine the personnel security policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. PS-1.3 Examine the personnel security procedures to determine if the procedures are sufficient to address all areas identified in the personnel security policy and all associated personnel security controls. PS-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel security policy and procedures control is implemented.	
PS-2	POSITION RISK DESIGNATION	P1 MOD PS-2	Control: The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [ASSIGNMENT: organization-defined frequency].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-2.1 Examine the organizational records or documents to determine if the organization: (i) establishes risk designations; (ii) assigns a risk designation to all organizational positions; (iii) follows screening criteria for individuals filling organizational positions; and (iv) reviews and revises position risk designations on an organization-defined frequency. PS-2.2 Test the position categorization procedures by comparing a list of organizational personnel and their clearance and/or authorization levels to the position risk designations to determine if the organization meets the screening criteria for those individuals filling the positions. PS-2.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the position categorization control is implemented.	
PS-3	PERSONNEL SCREENING	P1 MOD PS-3	Control: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [ASSIGNMENT: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-3.1 Examine organizational records or documents to determine if the organization appropriately screens individuals requiring access to organizational information and information systems prior to authorizing access. PS-3.2 Test the personnel screening process by comparing a list of organizational personnel requiring access to the information system and their associated screening dates to account creation dates to determine if the organization meets the screening criteria for those individuals. PS-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel screening control is implemented.	
PS-4	PERSONNEL TERMINATION	P1 MOD PS-4	Control: The organization, upon termination of individual employment: a. Disables information system access within [ASSIGNMENT: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [ASSIGNMENT: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [ASSIGNMENT: organization-defined personnel or roles] within [ASSIGNMENT: organization-defined time period].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-4.1 Examine organizational records or documents to determine if the organization: (i) revokes the information system accounts of terminated personnel; (ii) conducts exit interviews of terminated personnel; (iii) collects all information system-related property (e.g., keys, identification cards, building passes) of terminated personnel; and (iv) retains access to official documents and records on organizational information systems created by terminated personnel. PS-4.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel termination control is implemented. Control Enhancements: PS-4(2) Examine organizational records or documents to determine if the organization employs automated mechanisms to notify organization-defined personnel or roles upon termination of an individual.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
PS-5	PERSONNEL TRANSFER	P2 MOD PS-5	Control: The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [ASSIGNMENT: organization-defined transfer or reASSIGNMENT actions] within [ASSIGNMENT: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reASSIGNMENT or transfer; and d. Notifies [ASSIGNMENT: organization-defined personnel or roles] within [ASSIGNMENT: organization-defined time period].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-5.1 Examine organizational records or documents to determine if the organization: (i) reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and (ii) initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization. PS-5.2 Test the personnel transfer procedures of the organization by comparing the information system authorizations of current personnel to the access authorizations of transferred personnel to determine if all personnel have appropriate authorizations for the information system. PS-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel transfer control is implemented.	
PS-6	ACCESS AGREEMENTS	P3 MOD PS-6	Control: The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [ASSIGNMENT: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [ASSIGNMENT: organization-defined frequency].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-6.1 Examine organizational records or documents to determine if the organization: (i) 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 (ii) reviews and updates the access agreements on an organization-defined frequency. PS-6.2 Examine selected access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for the information system to determine if the access agreements are: (i) signed and retained in accordance with the documented organizational policy and procedures; and (ii) reviewed and updated by the organization on an organization-defined frequency. PS-6.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access agreements control is implemented.	
PS-7	THIRD-PARTY PERSONNEL SECURITY	P1 MOD PS-7	Control: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [ASSIGNMENT: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [ASSIGNMENT: organization-defined time period]; and e. Monitors provider compliance.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-7.1 Examine organizational records or documents to determine if the organization:(i) 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 applications, network and security management); and (ii) monitors thirdparty provider compliance to ensure adequate security. PS-7.2 Examine organizational records or documents to determine if the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35. PS-7.3 Interview selected organizational personnel with personnel security responsibilities to determine if the organization monitors third-party provider compliance with personnel security requirements. PS-7.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the third-party personnel security control is implemented.	
PS-8	PERSONNEL SANCTIONS	P3 MOD PS-8	Control: The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [ASSIGNMENT: organization-defined personnel or roles] within [ASSIGNMENT: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			PS-8.1 Examine organizational records or documents to determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. PS-8.2 Examine organizational records or documents including signed rules of behavior to determine if the organization defines and conveys the formal sanctions process to organizational personnel. PS-8.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel sanctions control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	P1 MOD RA-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [ASSIGNMENT: organization-defined frequency]; and 2. Risk assessment procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			RA-1.1 Examine organizational records or documents to determine if risk assessment policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. RA-1.2 Examine the risk assessment policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. RA-1.3 Examine the risk assessment procedures to determine if the procedures are sufficient to address all areas identified in the risk assessment policy and all associated risk assessment controls. RA-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment policy and procedures control is implemented.	
RA-2	SECURITY CATEGORIZATION	P1 MOD RA-2	Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			RA-2.1 Examine the system security plan to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST Special Publication 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization. RA-2.2 Interview selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners. RA-2.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented.	
RA-3	RISK ASSESSMENT	P1 MOD RA-3	Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [ASSIGNMENT: organization-defined document]]; c. Reviews risk assessment results [ASSIGNMENT: organization-defined frequency]; d. Disseminates risk assessment results to [ASSIGNMENT: organization-defined personnel or roles]; and e. Updates the risk assessment [ASSIGNMENT: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			RA-3.1 Examine organizational records or documents to determine if the organization assesses 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 its operations and assets (including information and information systems managed/operated by external parties). RA-3.2 Examine the risk assessment for the information system to determine if the assessment is consistent with NIST Special Publications 800-30 and 800-95. RA-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
RA-5	VULNERABILITY SCANNING	P1 MOD RA-5 (1)(2)(5)	b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [ASSIGNMENT: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [ASSIGNMENT: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancements: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. (2) The organization updates the information system vulnerabilities scanned [Selection (one or more): [ASSIGNMENT: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. (3) Not Selected.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			affecting the system are identified and reported. RA-5.2 Examine the latest vulnerability scanning results to determine if the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans. RA-5.3 Examine the latest vulnerability scanning results to determine if patch and vulnerability management is handled in accordance with NIST Special Publication 800-40 (Version 2). RA-5.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the vulnerability scanning control is implemented. Control Enhancements: RA-5(1) Examine organizational records or documents to determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned. RA-5(2) Examine organizational records or documents to determine if: (i) the organization defines the frequency of updates for information system vulnerabilities scanned; and (ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when new vulnerabilities are identified and reported. RA-5(5) Examine organizational records or documents to determine if: (i) the organization defines the list of information system components to which privileged access is authorized for selected vulnerability scanning activities;	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	P1 MOD SA-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [ASSIGNMENT: organization-defined frequency]; and 2. System and services acquisition procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-1.1 Examine organizational records or documents to determine if system and services acquisition policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. SA-1.1 Examine organizational records or documents to determine if system and services acquisition policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. SA-1.3 Examine the system and services acquisition procedures to determine if the procedures are sufficient to address all areas identified in the system and services acquisition policy and all associated system and services acquisition controls. SA-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and services policy and procedures control is implemented.	
SA-2	ALLOCATION OF RESOURCES	P1 MOD SA-2	Control: The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-2.1 Examine organizational records or documents to determine if the organization allocates, as part of its capital planning and investment control process, the resources required to adequately protect the information system consistent with NIST Special Publication 800-65. SA-2.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the allocation of resources control is implemented	
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	P1 MOD SA-3	Control: The organization: a. Manages the information system using [ASSIGNMENT: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-3.1 Examine organizational records or documents to determine if the organization manages the information system using a system development life cycle methodology that includes information security considerations. SA-3.2 Examine organizational records or documents to determine if the system development life cycle is consistent with NIST Special Publication 800-64. SA-3.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the life cycle support control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SA-4	ACQUISITION PROCESS	P1 MOD SA-4 (1) (2)(9) (10)	g. Acceptance criteria. Control Enhancements: (1) The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. (2) The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail]. (3) Not Selected. (4) Not Selected. (5) Not Selected. (6) Not Selected. (7) Not Selected. (8) Not Selected. (9) The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			organization's acquisition of commercial information technology products is consistent with NIST Special Publication 800-23. SA-4.3 Examine organizational records or documents to determine if references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST Special Publication 800-70. SA-4.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the acquisitions control is implemented. Control Enhancements: SA-4(1) Examine organizational records or documents to determine if the organization requires in acquisition documents that vendors/contractors provide information describing in the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. SA-4(2) Examine organizational records or documents to determine if the organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls. SA-4(9) Examine organizational records or documents to determine if the organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	
SA-5	INFORMATION SYSTEM DOCUMENTATION	P2 MOD SA-5	a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [ASSIGNMENT: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [ASSIGNMENT: organization	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-5.1 Examine organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel. SA-5.2 Examine organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. SA-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented. SA-5.6 Examine organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.	
SA-8	SECURITY ENGINEERING PRINCIPLES	P1 MOD SA-8	Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-8.1 Examine organizational records or documents to determine if the organization considers security design principles in the development and implementation of the information system consistent with NIST Special Publication 800-27. SA-8.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security design principles control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	P1 MOD SA-9(2)	Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [ASSIGNMENT: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis. Control Enhancements: (1) Not Selected. (2) The organization requires providers of [ASSIGNMENT: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-9.1 Examine organizational records or documents to determine if the organization ensures that third-party providers of information system services employ adequate security controls in the information systems providing such services in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. SA-9.2 Examine organizational records or documents to determine if 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. SA-9.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the outsourced information system services control is implemented. Control Enhancements: SA-9(2) Examine organizational records or documents to determine if the organization requires providers of organization-defined external information system services to identify the functions, ports, protocols, and other services required for the use of such services.	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	P1 MOD SA-10	Control: The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [ASSIGNMENT: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [ASSIGNMENT: organization-defined personnel].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-10 Examine organizational records or documents to determine if the organization requires that information system developers/integrators: (i) perform configuration management during information system: -design; -development; -implementation; and -operation; (ii) manage and control changes to the information system during: -design; -development; -implementation; and -modification; (iii) implement only organization-approved changes; (iv) document approved changes to the information system; and (v) track security flaws and flaw resolution.	
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	P1 MOD SA-11	Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [ASSIGNMENT: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SA-11.1 Examine the information system developer's organizational records or documents to determine if the developer creates a security test and evaluation plan, implements the plan, and documents the results. SA-11.2 Examine organizational records or documents to determine if the organization includes the developer's security test and evaluation results in the organization's Plan of Action and Milestones. SA-11.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the developer security testing control is implemented.	
SA-12	SUPPLY CHAIN PROTECTION	SELECTED FOR HIGH ONLY	Not Selected								
SA-13	TRUSTWORTHINESS	NOT SELECTED	Not Selected								
SA-14	CRITICALITY ANALYSIS	NOT SELECTED	Not Selected								

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	P1 MOD SC-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [ASSIGNMENT: organization-defined frequency]; and 2. System and communications protection procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-1.1 Examine organizational records or documents to determine if system and communications protection policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. SC-1.2 Examine the system and communications protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. SC-1.3 Examine the system and communications protection procedures to determine if the procedures are sufficient to address all areas identified in the system and communications protection policy and all associated system and communications protection controls. SC-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and communications protection policy and procedures control is implemented.	
SC-2	APPLICATION PARTITIONING	P1 MOD SC-2	Control: The information system separates user functionality (including user interface services) from information system management functionality.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-2.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information 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-2.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the application partitioning control is implemented.	
SC-3	SECURITY FUNCTION ISOLATION	SELECTED FOR HIGH ONLY	Not Selected								
SC-4	INFORMATION IN SHARED RESOURCES	P1 MOD SC-4	Control: The information system prevents unauthorized and unintended information transfer via shared system resources.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-4 Examine organizational records or documents to determine if the information system prevents unauthorized and unintended information transfer via shared system resources.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SC-5	DENIAL OF SERVICE PROTECTION	P1 MOD SC-5	Control: The information system protects against or limits the effects of the following types of denial of service attacks: [ASSIGNMENT: organization-defined types of denial of service attacks or reference to source for such information] by employing [ASSIGNMENT: organization-defined security safeguards].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-5.1 Examine organizational records or documents (including developer design documentation) to determine if the information system protects against or limits the effects of the organization-defined types of denial of service attacks. SC-5.2 Examine organizational records or documents to determine if the organization uses automated tools to protect against or limit the effects of organization-defined types of denial of service attacks. SC-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the denial of service protection control is implemented.	
SC-6	RESOURCE AVAILABILITY	NOT SELECTED	Not Selected								
SC-7	BOUNDARY PROTECTION	P1 MOD SC-7(3) (4) (5) (7)	Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture. Control Enhancements: (1) Not Selected. (2) Not Selected. (3) The organization limits the number of external network connections to the information system. (4) The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy [ASSIGNMENT: organization-defined frequency]; and removes exceptions that are no longer supported by an explicit mission/business need. (5) The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). (6) HIGH Only. (7) The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-7.1 Examine organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. SC-7.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary protection control is implemented. SC-7.5 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated. Control Enhancements: SC-7(3) Examine organizational records or documents to determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. SC-7(4) Examine organizational records or documents to determine if (i) the organization defines the frequency for reviewing exceptions to traffic flow policy; (ii) the organization implements a managed interface for each external telecommunication service; (iii) the organization establishes a traffic flow policy for each managed interface; (iv) the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (v) the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (vi) the organization reviews exceptions to the traffic flow policy in accordance with the organization-defined frequency; and (vii) the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. SC-7(5) Examine organizational records or documents to determine if (i) the information system, at managed interfaces, denies network traffic by default; and (ii) the information system, at managed interfaces, allows network traffic by exception. SC-7(7) Examine organizational records or documents to determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SC-8	TRANSMISSION INTEGRITY	P1 MOD SC-8 (1)	Control: The information system protects the integrity of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			organizational records or documents (including developer design documentation) to determine if the information system protects the integrity of transmitted information and how the integrity protections are implemented (i.e., mechanisms, tools, techniques, and technologies). SC-8.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that transmission integrity control is implemented. Control Enhancements: SC-8(1) Examine the information system documentation or test the information system to determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical	
SC-10	NETWORK DISCONNECT	P2 MOD SC-10	Control: The information system terminates the network connection associated with a communications session at the end of the session or after [ASSIGNMENT: organization-defined time period] of inactivity.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-10.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system terminates a network connection at the end of a session or after an organization-defined time period of inactivity and how the connection is terminated. SC-10.2 Test the network disconnection capability for the information system by leaving an open session for a specified amount of time to determine if the system terminates the network connection as expected. SC-10.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the network disconnect control is implemented.	
SC-11	TRUSTED PATH	NOT SELECTED	Not Selected								
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	P1 MOD SC-12	Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [ASSIGNMENT: organization-defined requirements for key generation, distribution, storage, access, and destruction].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-12.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information 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-12.2 Test the information system cryptographic key establishment and management by using the automated mechanisms to walk a test key through all the phases of its lifecycle from generation to revocation. SC-12.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic key establishment and management control is implemented. Control Enhancements: SC-12(1) Examine organizational records or documents to determine if the organization maintains availability of information in the event of the loss of cryptographic keys by users.	
SC-13	CRYPTOGRAPHIC PROTECTION	P1 MOD SC-13	Control: The information system implements [ASSIGNMENT: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-13.1 Examine organizational records or documents (including developer design documentation) to determine if the employed cryptography 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-13.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the use of validated cryptography control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SC-15	COLLABORATIVE COMPUTING DEVICES	P1 MOD SC-15	Control: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [ASSIGNMENT: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-15.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if 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) and how remote activation of collaborative computing is prohibited. SC-15.2 Test the information system by attempting to remotely control video or audio capabilities to determine if remote activation of collaborative computing mechanisms is restricted. SC-15.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the collaborative computing control is implemented.	
SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	NOT SELECTED	Not Selected								
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	P1 MOD SC-17	Control: The organization issues public key certificates under an [ASSIGNMENT: organization-defined certificate policy] or obtains public key certificates from an approved service provider.	Common Provided by VDC, if applicable			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-17.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system and how the policy is implemented in the information system. SC-17.2 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the public key infrastructure certificates control is implemented.	
SC-18	MOBILE CODE	P2 MOD SC-18	Control: The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-18.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if 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; (ii) documents, monitors, and controls the use of mobile code within the information system; and (iii) requires organizational officials to approve the use of mobile code. SC-18.2 Test the information system by attempting to run mobile code in an application where it is specifically prohibited to determine if the organization implements mobile code usage restrictions. SC-18.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the mobile code control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SC-19	VOICE OVER INTERNET PROTOCOL	P1 MOD SC-19	Control: The organization: a. 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 b. Authorizes, monitors, and controls the use of VoIP within the information system.	Common This control is most likely Not Applicable. Otherwise, Common			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-19.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; (ii) documents, monitors, and controls the use of VoIP within the information system; and (iii) requires organizational officials to approve the use of VoIP. SC-19.2 Test the VoIP capability by attempting to spoof or mask a caller's identity. SC-19.3 Test the VoIP capability by attempting to generate enough network volume to create a denial of service attack. SC-19.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the VoIP control is implemented.	
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	P1 MOD SC-20	Control: The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Common Provided by VDC and/or EDUCATE			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-20.1 Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing organizational information resources to entities across the Internet provides artifacts for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions and how the information system provides artifacts for data origin authentication and data integrity. SC-20.2 Test the information system by attempting to launch known attacks against the domain name servers. SC-20.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the secure name lookup service (authoritative source) control is implemented.	
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	P1 MOD SC-21	Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-21 Examine the information system documentation or test the information system to determine if the information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	P1 MOD SC-22	Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation..	Common Provided by VDC and/or EDUCATE			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-22 Examine the information system documentation or test the information system to determine if: (i) the information systems that collectively provide name/address resolution service for an organization are fault tolerant; and (ii) the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.	
SC-23	SESSION AUTHENTICITY	P1 MOD SC-23	Control: The information system protects the authenticity of communications sessions.	Common Provided by VDC			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-23 Test the information system configuration to determine if the information system provides mechanisms to protect the authenticity of communications sessions.	
SC-24	FAIL IN KNOWN STATE	SELECTED FOR HIGH ONLY	Not Selected								
SC-25	THIN NODES	NOT SELECTED	Not Selected								
SC-26	HONEYPOTS	NOT SELECTED	Not Selected								
SC-27	PLATFORM-INDEPENDENT APPLICATIONS	NOT SELECTED	Not Selected								

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SC-28	PROTECTION OF INFORMATION AT REST	P1 MOD SC-28	Control: The information system protects the [Selection (one or more): confidentiality; integrity] of [ASSIGNMENT: organization-defined information at rest].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SC-28 Examine organizational records or documents to determine if the information system protects the confidentiality and integrity of information at rest.	
SC-29	HETEROGENEITY	NOT SELECTED	Not Selected								
SC-30	CONCEALMENT AND DISDIRECTION	NOT SELECTED	Not Selected								
SC-31	COVERT CHANNEL ANALYSIS	NOT SELECTED	Not Selected								
SC-32	INFORMATION SYSTEM PARTITIONING	NOT SELECTED	Not Selected								
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	NOT SELECTED	Not Selected								

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	P1 MOD SI-1	Control: The organization: a. Develops, documents, and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [ASSIGNMENT: organization-defined frequency]; and 2. System and information integrity procedures [ASSIGNMENT: organization-defined frequency].	Common If additional system/application policy/procedures are in place, this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-1.1 Examine organizational records or documents to determine if system and information integrity policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required. SI-1.2 Examine the system and information integrity policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. SI-1.3 Examine the system and information integrity procedures to determine if the procedures are sufficient to address all areas identified in the system and information integrity policy and all associated system and information integrity controls. SI-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and information integrity policy and procedures control is implemented.	
SI-2	FLAW REMEDIATION	P1 MOD SI-2 (2)	Control: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [ASSIGNMENT: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. Control Enhancements: (1) HIGH ONLY. (2) The organization employs automated mechanisms [ASSIGNMENT: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-2.1 Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization identifies recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the information system. SI-2.2 Examine organizational records or documents to determine if 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. SI-2.3 Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures. SI-2.4 Examine organizational records or documents to determine if the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation. SI-2.5 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the flaw remediation control is implemented. Control Enhancements: SI-2(2) Examine organizational records or documents to determine if (i) the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation; and (ii) the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SI-3	MALICIOUS CODE PROTECTION	P1 MOD SI-3 (1) (2)	Control: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [ASSIGNMENT: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [ASSIGNMENT: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-3.1 Examine organizational records or documents to determine if the organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses). SI-3.2 Interview selected organizational personnel with system and information integrity responsibilities and examine malicious code protection mechanisms to determine if the mechanisms detect and eradicate malicious code transported: (i) by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes, or compact discs), or other common means; or (ii) by exploiting information system vulnerabilities. SI-3.3 Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software). SI-3.4 Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational policy and procedures. SI-3.5 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the malicious code protection control is implemented. Control Enhancements: SI-3(1) Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization centrally manages malicious code protection mechanisms employed in organizational information systems. SC-3(2)	
SI-4	INFORMATION SYSTEM MONITORING	P1 MOD SI-4 (2) (4) (5)	Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [ASSIGNMENT: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [ASSIGNMENT: organization-defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [ASSIGNMENT: organization-defined information system monitoring information] to [ASSIGNMENT: organization-defined personnel or roles] [Selection (one or more): as needed; [ASSIGNMENT: organization-defined frequency]]. Control Enhancements: (1) Not Selected. (2) The organization employs automated tools to support near real-time analysis of events. (3) Not Selected. (4) The information system monitors inbound and outbound communications traffic [ASSIGNMENT: organization-defined frequency] for unusual or unauthorized activities or conditions. (5) The information system alerts [ASSIGNMENT: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [ASSIGNMENT: organization-defined compromise indicators].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-4.1 Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools. SI-4.2 Examine intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies. SI-4.3 Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures. SI-4.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SI-5	SECURITY ALERTS, ADVISORIES AND DIRECTIVES	P1 MOD SI-5	Control: The organization: a. Receives information system security alerts, advisories, and directives from [ASSIGNMENT: organization-defined external organizations] on an ongoing basis; b. b. Generates internal security alerts, advisories, and directives as deemed necessary; c. c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [ASSIGNMENT: organization-defined personnel or roles]; [ASSIGNMENT: organization-defined elements within the organization]; [ASSIGNMENT: organization-defined external organizations]]; and d. d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-5.1 Examine organizational records or documents (including any logs documenting alerts/advisories) to determine if the organization: (i) receives information system security alerts and advisories; (ii) disseminates the alerts and advisories to appropriate personnel; (iii) takes appropriate actions in response; and (iv) documents the results including the date and time of each action taken. SI-5.2 Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization provides the capability to immediately react and respond to new security alerts and advisories. SI-5.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security alerts and advisories control is implemented. Control Enhancements: SI-5(1) Examine organizational records or documents to determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization.	
SI-6	SECURITY FUNCTION VERIFICATION	SELECTED FOR HIGH ONLY	Not Selected								
SI-7	SOFTWARE FIRMWARE AND INFORMATION INTEGRITY	P1 MOD SI-7 (1) (7)	Control: The organization employs integrity verification tools to detect unauthorized changes to [ASSIGNMENT: organization-defined software, firmware, and information]. Control Enhancements: (1) The information system performs an integrity check of [ASSIGNMENT: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [ASSIGNMENT: organization-defined transitional states or security-relevant events]; [ASSIGNMENT: organization-defined frequency]]. (2) Not Selected. (3) Not Selected. (4) Not Selected. (5) Not Selected. (6) Not Selected. (7) The organization incorporates the detection of unauthorized [ASSIGNMENT: organization-defined security-relevant changes to the information system] into the organizational incident response capability.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-7 Examine organizational records or documents to determine if the information system detects unauthorized changes to software and information. Control Enhancements: SI-7(1) Examine organizational records or documents to determine if: (i) the organization defines the frequency of integrity scans to be performed on the information system; and (ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency. SI-7(7) Examine organizational records or documents to determine if the organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability.	
SI-8	SPAM PROTECTION	P1 MOD SI-8	Control: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. Control Enhancements: (1) The organization centrally manages spam protection mechanisms. (2) The information system automatically updates spam protection mechanisms.	Common Provided by VDC			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-8.1 Examine organizational records or documents to determine if the organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. SI-8.2 Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail. SI-8.3 Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures. SI-8.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the spam protection control is implemented. Control Enhancements: SI-8(1) Examine organizational records or documents to determine if the organization centrally manages spam protection mechanisms. SI-8(2) Examine the information system configuration settings to determine if the information system automatically updates spam protection mechanisms (including signature definitions).	
SI-10	INFORMATION INPUT VALIDATION	P1 MOD SI-10	Control: The information system checks the validity of [ASSIGNMENT: organization-defined information inputs].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-10.1 Examine the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible. SI-10.2 Examine the information system to determine if 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. SI-10.3 Examine the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands. SI-10.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.	

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
SI-11	ERROR HANDLING	P2 MOD SI-11	Control: The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [ASSIGNMENT: organization-defined personnel or roles].	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-11.1 Examine the information system to determine if the system identifies and handles error conditions in an expeditious manner. SI-11.2 Examine the information system to determine if the system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries. SI-11.3 Examine the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel). SI-11.4 Examine the information system to determine if the system lists sensitive information (e.g., account numbers, social security numbers, and credit card numbers) in error logs or associated administrative messages. SI-11.5 Interview selected organizational personnel with system and information integrity responsibilities to determine if the information system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures. SI-11.6 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the error handling control is implemented.	
SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	P2 MOD SI-12	Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	Common, Hybrid, System-Specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			SI-12.1 Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization retains output from the information system in accordance with organizational policy and operational requirements/procedures. SI-12.2 Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization handles output from the information system in accordance with: (i) labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output; and (ii) organizational policy and operational requirements/procedures. SI-12.3 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information output handling and retention control is implemented.	
SI-13	PREDICTABLE FAILURE PREVENTION	NOT SELECTED	Not Selected								

Security Control Information					Control Assessment Information						
NIST Security Control Number	**Security Control Name**	**Priority / Baseline Allocation**	**Security Control and Enhancements**	**Security Control Type** (verify this type)	**Last Date Security Control Assessed**	**Assessor Information**	**Assessed Security Control Effectiveness** (select one of the following)	**Findings / Deficiencies Found**	**Scoping Guidance/ Risk -Based Decision Justification** (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	**NIST 800-53A Assessment Steps Used**	**Assessment Evidence**
AR-2	PRIVACY IMPACT AND RISK ASSESSMENT	No priority information / All baselines	The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.	Hybrid System-specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AR-2.1 Examine organizational records or documents to determine if a PIA has been completed and approved	
AR-4	PRIVACY MONITORING AND AUDITING	No priority information / All baselines	The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.	System-specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AR-4.1 Examine organizational documentation to determine if privacy controls are monitored and assessed regularly to ensure effective implementation	
AR-7	PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT	No priority information / All baselines	The organization designs information systems to support privacy by automating privacy controls.	System-specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AR-7.1 Examine the information system documentation and configuration to determine if automated privacy controls are in place.	
DI-1	DATA QUALITY	No priority information / All baselines	The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	Hybrid System-specific			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			DI-1.1 Examine organizational records or documents to determine if a Systems of Records Notice (SORN) has been completed and approved DI-1.2 Examine system procedures to determine if the system has automated data integrity checks or if there are procedures in place to review and correct PII	