## Access Control (AC)

### AC-1 Access Control Policy and Procedures Requirements (L) (M)

The organization:

1. 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
2. Reviews and updates the current:
   1. Access control policy [FedRAMP Assignment: at least every 3 years]; and
   2. Access control procedures [FedRAMP Assignment: at least annually].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: All | |
| Parameter AC-1(a): All | |
| Parameter AC-1(b)(1): at least annually | |
| Parameter AC-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | See Below |
| Part b1 | AC Policies are reviewed as part of the annual security assessment |
| Part b2 | AC Procedures are reviewed as part of the annual security assessment |

### AC-2 Account Management (L) (M)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. 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;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
7. Monitors the use of information system accounts;
8. Notifies account managers:
9. When accounts are no longer required;
10. When users are terminated or transferred; and
11. When individual information system usage or need-to-know changes;
12. 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;
13. Reviews accounts for compliance with account management requirements [FedRAMP Assignment: at least annually]; and
14. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: All | |
| Parameter AC-2(a): Infrastructure Accounts (LDAP, Active Directory, Proxy Servers, DNS), Network Administrator Accounts (switches, routers, firewalls), Server Administrator Accounts (including accounts with SUDO permissions), Database Administrator Accounts, Service Accounts, Limited Administrator Accounts, Developer Accounts, User Support Team Accounts, User Accounts (standard user accounts) | |
| Parameter AC-2(e): System Owner | |
| Parameter AC-2(f): Account Creation and Management Process | |
| Parameter AC-2(j): Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Infrastructure Accounts (LDAP, Active Directory, Proxy Servers, DNS) Accounts of this type have authorization to make changes to critical infrastructure components that may affect the availability or security of multiple systems in the environment. Access to these kinds of accounts should be strictly controlled and all activity should be logged. Accounts of this type are considered privileged accounts. Access to these accounts requires the approval of the Technology Services Lead and the ISSO. Network Administrator Accounts (switches, routers, firewalls) Accounts of this type have administrative control including the ability to make changes of all network devices (switches, firewalls, vpn, etc). Access to these kinds of accounts should be strictly controlled and all activity should be logged. Accounts of this type are considered privileged accounts. Access to these accounts requires the approval of the Network Lead and the ISSO. Server Administrator Accounts (including accounts with SUDO permissions) Accounts of this type have administrative control of one or more servers including the ability to make changes to both the content and configuration of the server. Some configuration settings may be configured and enforced by policies controlled at the Infrastructure level (i.e. group policies in Windows). Accounts should be granted access only to those servers needed to perform job functions. Accounts of this type are considered privileged accounts. All activities of these accounts should be logged. Access to these accounts requires the approval of the System Owner. Database Administrator Accounts Accounts of this type have administrative control of one or more database including the ability to make changes to both the content and configuration of the database. Some configuration settings may be configured and enforced by policies controlled at the Infrastructure or server level (i.e. group policies in Windows or password complexity policies). Accounts should be granted access only to those databases needed to perform job functions. All activities of these accounts should be logged. Accounts of this type are considered privileged accounts. Access to these accounts requires the approval of the System Owner and the Database Team Lead. Service Accounts Accounts of this type are used to run automated scripts and applications in either an unattended and persistent fashion, or for deployment of specific shared objects. Service accounts should be created for an explicit purpose and should have only the authorization needed to perform that purpose. A single service accounts should never be used for multiple applications. Service accounts should, when possible, be configured such that they cannot be used to logon to an interactive session. Service account passwords must be of the strongest complexity and generated randomly. Each service account must have a designated owner who is responsible for maintaining the integrity of the account credentials, ensuring the account is not used for anything besides it’s intended purpose, and for notifying the DMT when the account is no longer needed. Accounts of this type are not normally considered privileged accounts, but may be designated as privileged if the account has authorizations similar to a privileged account type.. Creation of a service account requires approval from the Data Management team Lead, the System Owner(s) for which the account will have access, and the ISSO. Limited Administrator Accounts Accounts of this type can modify some settings and files on a limited set of servers under controlled circumstances.  Accounts of this type are not considered privileged accounts. Access to these accounts is determined by the System Owner. Developer Accounts This account type has full access to a sandbox development server and the test environment for prototyping and application testing. Access to the production sites is limited to read-only access and should be used to perform tasks such as troubleshooting or monitoring. Accounts of this type are not considered privileged accounts. Access to these accounts is determined by the Application Team Lead and the System Owner. MAX Support Team Accounts These accounts have access to the MAX Security application to manage MAS accounts. This tool has great power to control the roles, groups, and effective authorization of other accounts. Accounts of this type are not considered privileged accounts. Access to these accounts is determined by the MAX Support Team Lead MAX Authentication Services (MAS) Accounts (standard [max.gov](http://max.gov/) user accounts) These accounts are provided to both internal and external users for accessing the [MAX.gov](http://max.gov/) SaaS offerings as well as other information systems which use [MAX.gov](http://max.gov/) as a service. Accounts are categorized into two groups, Federal accounts which have access to unrestricted content within the [MAX.gov](http://max.gov/) environment and Non-Federal accounts which have access ONLY to information that is explicitly granted to them. Accounts of this type are not considered privileged accounts. |
| Part b | User accounts, regardless of the role(s) assigned, must be issued to a single user and may never be shared between multiple users. Service accounts should be assigned a specific owner and to the extent possible should be used only by applications or automated processes and not by individual users. |
| Part c | Conditions for group/role membership are defined by the System Owner in coordination with the ISSO. Organizational requirements for some roles (i.e., must possess a secret clearance in order to directly manage MAX GSS systems) are determined by the ISSO in conjunction with the MAX Policy Lead and are enforced by the System Owner. |
| Part d | Infrastructure and Network Administrator Accounts  * + Successful FBI SSBI investigation, and the user is clearable to at least Secret or be an approved customer   + Approval from Contracting Officer, Project Manager, or customer of resource, or   + Need for system access as identified through job role and access requested by Project manager or customer   + In special circumstances direct approval from the System Owner of [MAX.gov](http://max.gov/)   + Additional requirements imposed by the System Owner |
| Part e | System Owners may approve accounts individually or by defining objective criteria. For example, a System owner could approve accounts for all employees of an agency or all personnel assigned to a particular contract task order. |
| Part f | Detailed instructions to create, enable, modify, disable, and remove information system accounts is provided in the Account Creation and Management Process. This process provides specific guidance for creating accounts within specific Information Systems (LDAP, Active Directory, etc.) and also documents the requirements for authorizing an account to specific information systems. |
| Part g | The components within the information system must be configured to monitor privileged account access including login failures via audit logs in Linux and Security Log in Windows. All logs are collected by the core audit server, Splunk. The ISSO will regularly review privileged account activity. |
| Part h | The ISSO and the Operations Team lead must be notified of any change in staffing including removal of a user from a project or task. The ISSO and Operations Team Lead are responsible for adjusting the roles assigned to a user’s account or terminating the account as needed. |
| Part i | All accounts and permissions in the information system must be deployed in compliance with a Least  Privilege philosophy. Accounts should be issued for a specific individual OR a specific purpose. Account re-ruse by multiple applications or individuals should be avoided unless absolutely necessary.  To ensure accounts have all the permissions they require and only the permissions they require, roles must be created within information system components. Permissions to perform operations or access data must be mapped to roles and users must be assigned to these roles. Accounts should be assigned to roles as required for job functionality. Permissions should never be granted to individual accounts unless absolutely necessary. All accounts, roles, and permissions should be reviewed regularly to ensure that they are still appropriate and being used as intended. |
| Part j | The Account Management Team performs account reviews on a monthly basis for User accounts. User accounts are reviewed for activity. If no activity is reported for 12 consecutive months the Account Management Team will attempt to contact the Account Owner to determine if the account is still needed.  Non-Federal accounts must have a valid sponsor. If the sponsor’s account is closed for any reason, the owner of the Non-Federal account will be notified via email that they have 30 days to identify a new sponsor or their account will be closed.  The Operations Team Lead and the ISSO review all privileged accounts at least annually. Accounts are reviewed for activity and may be disabled or deleted if no activity is detected after consulting with the account owner. Account authorizations are also reviewed and may be revoked if they are no longer needed after consulting with the account owner.  All service accounts are reviewed monthly by the Operations Team Lead and/or the Database Team lead. Accounts are reviewed for activity and may be disabled or deleted if no activity is detected after consulting with the account owner. Account authorizations are also reviewed and may be revoked if they are no longer needed after consulting with the account owner. |
| Part k | Users should never share credentials for their user accounts. For Service accounts, credentials should be closely managed and shared only when absolutely critical. If a user with knowledge of a service account credential leaves the organization then the credential must be changed within 24 hours. If a credential is potentially compromised (e.g. it is sent unencrypted in an email) the credential should be immediately reset and a security incident should be recorded. |

#### AC-2 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the management of information system accounts.

| AC-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Technology Services | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (1) What is the solution and how is it implemented? |
| --- |
| Management of accounts is currently managed manually. The relatively small number of internal accounts makes this manageable, but automated solutions are planned for the future. |

#### AC-2 (2) Control Enhancement (M)

The information system automatically [Selection: removes; disables] temporary and emergency accounts after [FedRAMP Assignment: no more than 30 days for temporary and emergency account types].

| AC-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter AC-2(2)1: N/A | |
| Parameter AC-2(2)2: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (2) What is the solution and how is it implemented? |
| --- |
| Temporary and emergency accounts are not permitted within the information system. Instead, users create a normal user account which is then granted necessary privileges. Privileges are revoked when no longer required as specified in AC-03. |

#### AC-2 (3) Control Enhancement (M)

The information system automatically disables inactive accounts after [FedRAMP Assignment: ninety (90) days for user accounts].

AC-2 (3) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Joint Authorization Board (JAB)/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Responsible Role: User Account Team | |
| Parameter AC-2(3): 1 year for external users and 1 Month for internal accounts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (3) What is the solution and how is it implemented |
| --- |
| The Account Management Team performs account reviews on a monthly basis for User accounts. User accounts are reviewed for activity. If no activity is reported for 12 consecutive months the Account Management Team will attempt to contact the Account Owner to determine if the account is still needed.  Activity for privileged accounts is reviewed Monthly by the ISSO and Operations team lead. Inactive accounts may be disabled or have unused roles revoked after consultation with the account owner. |

#### AC-2 (4) Control Enhancement (M)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

| AC-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AC-2(4): Information Assurance Team | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (4) What is the solution and how is it implemented? |
| --- |
| The components within the information system must be configured to monitor account creation, modification, enabling, disabling, and removal actions for privileged accounts via audit logs in Linux and Security Log in Windows. All logs are collected by the core audit server, Splunk.  The IA Team will regularly review privileged account activity. |

#### AC-2 (5) Control Enhancement (M)

The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].

AC-2 (5) Additional FedRAMP Requirements and Guidance:

Guidance: Should use a shorter timeframe than AC-12

| AC-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Operations Team Lead | |
| Parameter AC-2(5): 30 minutes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (5) What is the solution and how is it implemented? |
| --- |
| Users shall be prompted with an alert or pop-up message after 30 minutes of inactivity. The specific language and design may be determined by the system component. But the message content must include an option for the user to log-off ending their session. |

#### AC-2 (7) Control Enhancement (M)

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.

| AC-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Operations Team Lead | |
| Parameter AC-2(7)(c): action to remove the user form the no longer required role | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

#### AC-2 (9) Control Enhancement (M)

The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].

AC-2 (9) Additional FedRAMP Requirements and Guidance:

Required if shared/group accounts are deployed.

| AC-2 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter AC-2(9): N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
| User accounts, regardless of the role(s) assigned, must be issued to a single user and may never be shared between multiple users. Service accounts should be assigned a specific owner and to the extent possible should be used only by applications or automated processes and not by individual users. |

#### AC-2 (10) Control Enhancement (M) (H)

The information system terminates shared/group account credentials when members leave the group.

AC-2 (10) Additional FedRAMP Requirements and Guidance:

Required if shared/group accounts are deployed.

| AC-2 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
| User accounts, regardless of the role(s) assigned, must be issued to a single user and may never be shared between multiple users. Service accounts should be assigned a specific owner and to the extent possible should be used only by applications or automated processes and not by individual users. |

#### AC-2 (12) Control Enhancement (M)

The organization:

1. Monitors information system accounts for [Assignment: organization-defined atypical use]; and
2. Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].

AC-2 (12) (a) and AC-2 (12) (b) Additional FedRAMP Requirements and Guidance:

Required for privileged accounts.

| AC-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AC-2(12)(a): excessive failed login attempts | |
| Parameter AC-2(12)(b): Information Assurance Team | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The components within the information system must be configured to monitor privileged account access including login failures via audit logs in Linux and Security Log in Windows. All logs are collected by the core audit server, Splunk. |
| Part b | The IA Team will regularly review privileged account activity. |

### AC-3 Access Enforcement (L) (M) (H)

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

| AC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO and/or System Owner; MAX.gov (internal users) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| Accurate enforcement of appropriate system access is essential in protecting the information system against vulnerabilities, threats (both internal and external), and compromise of security controls. Shared responsibility for implementation of Access Enforcement Policy Access enforcement is applicable to internal and external users.  In the case of external users, assignment of roles and privileges is normally the responsibility of other external users.  In order to ensure that integrity, confidentiality, and availability are equally protected; users should, to the extent possible, be allowed to manage and control access to data for which the user has access.  This allows the data owner, who is most familiar with the information, to control access rather than a central system administrator, who may prevent necessary access due to competing priorities or could be tricked into providing unnecessary access through social engineering.  [The](http://max.gov/) Service Provider remains responsible for enforcement of access restrictions and privileges within the information system.  For internal users, [The](http://max.gov/) Service Provider is responsible for the assignment of roles and privileges as well as enforcing access restrictions and privileges within the information system. Policy for Access Enforcement for information system account users**1.**Identity Verification Whenever possible, Identity Verification should be achieved using a secure two-factor methodology with the highest preference being given to using PIV cards as the second factor.  At a minimum, a unique user ID and password must be used to identify a user to a particular system or object.  Shared or Service accounts are permitted only when essential to support operational requirements.  The policy for establishing a service account can be found in the Access Control (AC-2) policy **2.**Multi-Layer Access Enforcement To the extent possible, access restrictions must be enforced at each layer of the information system.  Access enforcement rules should be defined based on user roles.  Once a user has been granted a specific role, the privileges and restrictions assigned to that role must be enforced at both the application and data layers.  The Information System should operate on a Zero-Trust model and should verify a user’s privileges at each step of an operation.  A user’s ability to request an action may NEVER be used to assert that the user has permissions to perform that action. **3.**Encryption of Privileged Data To prevent a user from leveraging one form of privileged access to access data or functions for which the user is not authorized (commonly referred to as privilege escalation) data at rest should be encrypted using a FIPS 140-2 compliant and NIST validated encryption standard.  The rigor with which this requirement is implemented should be commensurate with the value of the data being protected.  Full requirements for and guidance on selecting encryption modules can be found in NIST Publication FIPS 140-2 (<https://csrc.nist.gov/publications/detail/fips/140/2/final>) **4.**Restrictions on Anonymous or Public Access Operating system controls must be configured to disable public access to all system files, objects, and directories.  Configure operating system controls to disable public "read" access to files, objects, and directories that contain sensitive information.  Databases and other applications should reject anonymous connection requests **5.**Restrictions on Granting Privileged Access directly to user accounts To ensure compliance and to minimize the risk of error, privileges should never be granted to individual user accounts.  Privileges should always be granted to system-defined roles to which accounts are then assigned.  This provides for more effective monitoring of privileges assigned to both objects and users. |

### AC-4 Information Flow Enforcement (M) (H)

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*].

| AC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AC-4: external network connections, internal subnets, VLANs, and Network Objects | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-4 What is the solution and how is it implemented? |
| --- |
| The flow of information between systems is a key requirement in ensuring that the confidentiality of data is maintained by protecting it from accidental disclosure. To ensure compliance, both the ISSO and SO must approve any exceptions to this policy.  The organization shall deploy mechanisms to control access to the Information System’s network backbone and/or routed infrastructure. The Information System Network must be configured to monitor and control communications at the external boundary of the network and internal boundaries at strategic locations.  The Information System Network must connect to external networks or information systems only through managed interfaces approved by the System Owner and the ISSO. These managed interfaces must consist of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels, web content filters, data loss prevention) arranged in accordance with an effective security architecture.  Protective controls shall at a minimum include the following:   1. Positive source and destination address checking to restrict rogue networks from manipulating the Information System’s routing tables. 2. Authentication to ensure that routing tables do not become corrupted with false entries. 3. Use network address translation (NAT) to obfuscate internal network addresses. 4. Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to accomplish the mission of the Information System.   Managing Information Flow  Network Layer  At the network layer, firewalls and switches must be configured to enforce boundary separation between internal security boundaries.  Network traffic flow must describe the logical connections between systems.  The system enforces separation using a combination of logical and physical separation between systems using switches and VLANs:   * 1. VLANs are used in combination with firewall rules to enforce logical separation between networks (management, hypervisor, security, and internal), to ensure that data cannot be transferred between the security boundaries outside of approved channels.   2. Physical separation is enforced between IaaS customers and the internal network using switches.  With each, switch connecting through a firewall that will only allow approved data flows to enter or exit each network.   3. Internet traffic is routed through the external proxies, which exist on dedicated hypervisors.   System Layer  At the system layer, the servers should be grouped by business purpose rather than operational purposes such as applications, databases, file servers, etc. servers should be grouped such that the application, database, and file servers for a particular business function are grouped together and then isolated from each other as needed. This configuration minimizes the risk of lateral movement between business systems in the event of a compromise. System level firewalls should be enabled allowing only data flows that relate to the purpose of the system, to prevent connections that will violate this policy.  Application Layer  At the application layer, each application should be configured to enforce access only to specific systems on specific ports.  If possible, data transfers should be limited to specific data formats (XML, JSON, text, etc.).   * 1. If required, the application must be explicitly configured to utilize the proxy server as the gateway that provides inbound and outbound connections to the internet.   2. Applications are required to document connections that move beyond the system boundary.   3. The information system manages information flow based on the information system boundary.   Important Considerations   1. The system must enforce information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decision. 2. System must be configured to prevent encrypted data from bypassing content-checking mechanisms. 3. System must enforce defined limitations on the embedding of data types. 4. System must enforce information flow control on metadata (monitor communications that occur within the system). 5. System will enforce the use of human review for system security when the system does not perform as expected. 6. The information system must be configured to identify and validate sources and destinations of information transfer. 7. The system must create labels for data to differentiate between system specific components and individuals involved in preparing, sending, and receiving information. |

#### AC-4 (21) Control Enhancement (M) (H)

The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

| AC-4 (21) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AC-4(21)-1: virtual or physical switches and firewalls | |
| Parameter AC-4(21)-2: restricting lateral movement and protecting network backbone components from attack by a compromised edge device | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
| Lateral movement must be managed when possible by information flow enforcement at the point of origin, destination and at least one other inline device. Access to management ports and network backbone devices must be permitted only from well protected management servers which require multi-factor authentication. |

### AC-5 Separation of Duties (M) (H)

The organization:

1. Separates [*Assignment: organization-defined duties of individuals*];
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Section Error: Reference source not found Error: Reference source not found.

| AC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Management (Organization) and Employees (Users) | |
| Parameter AC-5(a): duties such that , a user may not be assigned to a role that is in part or in whole responsible for auditing or approving any other tasks performed by that user. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Separating duties of individuals:  **Prime Directive**: Individual duties must be separated to prevent conflicts of interest. It is expected that a user may have multiple roles. Generally speaking, a user may not be assigned to a role that is in part or in whole responsible for auditing or approving any other tasks performed by that user. For example, a project manager may also be a member of the change management board but must not unilaterally approve changes submitted by the team they manage.  In addition to this general guidance, roles and responsibilities for system users must be assigned as follows:   1. The Information System should define roles for each mission function and privileged access should be assigned to users ONLY through the assignment of the user’s account to the respective role. Roles must be defined at the most granular level required to enforce approved separation of duties policies and procedures. For example, if it is determined that a user should be granted some but not all of the access currently assigned to a given role, a new role should be created which reflects the required permissions. 2. Different individuals should perform related information system support functions (e.g., system management and network security or systems programming and testing) when possible. For example, a developer may be assigned the tester role and the developer role on a given project due to resource constraints. The developer cannot test his or her own code as that would be a violation of the Prime Directive. The user could provide testing approval for other developer’s code. While this situation would be permissible, it is not ideal and should be avoided when possible. 3. Users who administer access control functions must not administer audit functions.   There must be different administrator accounts for different roles. The use of a shared account inherently defines all users with access to that account as sharing a role. |
| Part b | The system owner must ensure a well-documented outline of the roles and responsibilities of the information system users is maintained and available. This shall be used as a system user guide for access configuration to allow appropriate access to the system. |
| Part c | The system must be configured to implement the appropriate access authorizations for individual users. This will normally be accomplished by assigning permissions to defined user roles and then assigning users to those roles.  Procedures should be implemented to prevent a user being assigned to a role that would create a conflict with an existing role. |

### AC-6 Least Privilege (M) (H)

The organization employs the principle 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.

| AC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Approving authorities | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 What is the solution and how is it implemented? |
| --- |
| Enforcement of least privilege access control practices protects sensitive information and limits the damage that can result from accident, error, or unauthorized use. Least privilege practices must be applied not only at the account/user level but should also be considered when executing information system processes. Processes should be executed by accounts that possess only the minimum privileges necessary. This is especially important with unattended processes such as scheduled jobs or always on services such as a web server. Care should be taken in configuring these services so that if the service is compromised or misconfigured the risk to the information system is minimized. System Access Restrictions  1. Disable all file system access not explicitly required for system, application, and administrator functionality. 2. Logical and physical access to sub-contractors or third party users should be restricted in the same way as other internal users and must additionally be restricted to the specific period of time for which access is required. Sub-contractors or third party users must agree to comply with the information system security requirements. The selection process for contractors, vendors or other supporting service providers must consider the organization's ability to adhere to and support the information system security policy. 3. Restrict the use of database management utilities to only authorized database administrators.  Prevent users from accessing database data files at the logical data view, field, or field-value levels.  Implement column-level access controls. 4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties. 5. Access to data should be enforced at every level of the application stack. Redundant access controls should be built in at the data, application, and view layers. Obfuscation is never a substitute for access control. |

#### AC-6 (1) Control Enhancement (M)

The organization explicitly authorizes access to [organization defined security functions or security relevant information whether it is deployed in hardware, software or firmware].

| AC-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Technology Services Team Lead, System Owner, ISSO | |
| Parameter AC-6(1): audit logs and auditing behavior, boundary protection system rules, configuring/modifying access authorizations (i.e., permissions, privileges) for other users that could be leveraged to circumvent other access controls, authentication parameters, system configurations and parameters, and system-level software, administrator tools, scripts and utilities | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
| Only the Technology Services Team Lead, the System Owner, or the ISSO may authorize a user to be granted any of the following permissions:   1. Setting/modifying audit logs and auditing behavior 2. Setting/modifying boundary protection system rules 3. Configuring/modifying access authorizations (i.e., permissions, privileges) for other users that could be leveraged to circumvent other access controls. Examples include root, Domain Admin, or other super user accounts including highly privileged accounts at the application layer 4. Setting/modifying authentication parameters 5. Setting/modifying system configurations and parameters 6. Setting/modifying/configuring system-level software, administrator tools, scripts and utilities |

#### AC-6 (2) Control Enhancement (M) (H)

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing non-security functions.

AC-6 (2) Additional FedRAMP Requirements and Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

| AC-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Administrators | |
| Parameter AC-6(2): audit logs and auditing behavior, boundary protection system rules, configuring/modifying access authorizations (i.e., permissions, privileges) for other users that could be leveraged to circumvent other access controls, authentication parameters, system configurations and parameters, and system-level software, administrator tools, scripts and utilities | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Date of Authorization , | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
| Users maintain a separate account with reduced privileges and escalate to the highly privileged accounts when necessary. |

#### AC 6 (5) Control Enhancement (M) (H)

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

| AC-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter AC-6 (5): users after the successful adjudication of a Tier 3 and Tier 5 investigation | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
| Privileged accounts on the information system may be granted only to users after the successful adjudication of a Tier 3 Investigation (T3) formerly National Agency Check with Local Agency Check and Credit (NACLC), Tier 5 Investigation (T5) formerly Single Scope Background Investigation (SSBI), or equivalent. |

#### AC-6 (9) Control Enhancement (M) (H)

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: Administrators, Developers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
| The information system must log any use of privileged accounts, or roles, for the following functions:   1. Setting/modifying audit logs and auditing behavior; 2. Setting/modifying boundary protection system rules; 3. Configuring/modifying access authorizations (i.e., permissions, privileges); 4. Setting/modifying authentication parameters; and 5. Setting/modifying system configurations and parameters   The system users must follow the concept of least privilege for specific duties and information systems. This include specific ports, protocols, and services in accordance with risk assessments as necessary to adequately mitigate risk to the system’s operation, assets and individuals. |

#### AC-6 (10) Control Enhancement (M) (H)

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

| AC-6 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: Administrators, Developers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
| The information system must prevent non-privileged users from executing privileged functions to disable, circumvent, or alter implemented security safeguards/countermeasures. Enforcement of the requirements in this policy must be integrated into the information system and may not be enforced solely by administrative policy. |

### AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

1. Enforces a limit of [FedRAMP Assignment: not more than three (3)] consecutive invalid logon attempts by a user during a [FedRAMP Assignment: fifteen (15) minutes]; and
2. 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.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Application owners and system’s ISSO | |
| Parameter AC-7(a)-1: 3 | |
| Parameter AC-7(a)-2: before account is locked and password must be reset | |
| Parameter AC-7(b)-1: Locks | |
| Parameter AC-7(b)-2: until password is reset | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The restrictions resulting from unsuccessful logon attempt should be enforced at the operating system and application. Specific parameters defined in this policy may vary depending on the system type, information sensitivity, and role of the account. For all accounts on any system, the following parameters must be defined: Number of failed Logon attempts permitted before action is taken Application Owners in coordination with the system ISSO must determine the appropriate number of logon attempts to allow before an action is taken. Configuration of the information system must ensure that the system will track the number of failed logon attempts and implement the designated action when the threshold is exceeded.  The number of permitted logon attempts must be determined with consideration for the mission of the user(s), the sensitivity of the information system, and the sensitivity of the information stored by the system.  Absent any other considerations, the recommended limit is three consecutive failed logon attempts. |
| Part b | Implementation of Account Lock The system must be configured to automatically lock the account once the allowed number of failed logon attempts has been exceeded. A user shall not be able to logon to any information system using a locked account. How long the account is locked and how the lock can be resolved should be determined by the Application Owners in coordination with the system ISSO . Having the lock expire after a fixed period of time is acceptable, provided that the duration of the lock is sufficient to dissuade an attacker. Locking the account until the user performs an action such as a password reset or contacting an administrator is also acceptable absent any other considerations, the recommended duration of the account lock is 1 hour. Important Considerations for Unsuccessful Logon Attempt Due to the potential for denial of service care must be taken in selecting account lockout parameters. Preference should be shown to configurations that allow a user to unlock a disabled account by re-verifying their identity using the credentials originally associated with the account creation. |

### AC-8 System Use Notification (L) (M) (H)

The information system:

1. 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;
2. 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
3. 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.

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Administrators, Developers | |
| Parameter AC-8(a): Displays an approved system use notification message or banner which must be acknowledged by the user | |
| Parameter AC-8(c)-1: Visible notification | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system must be configured to display approved system security and privacy statements which are consistent with Executive Orders, federal laws, directives, regulations, or standards such as:   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. 4. Use of the information system indicates consent to monitoring and recording. |
| Part b | The notification message or banner must be retained on the screen until the user acknowledges the usage conditions. The banner or message must provide privacy and security notices before granting system access:   1. The information system must be configured to ensure that logon or access is restricted until the user has read, accepted, and consented to the privacy or the security message that is displayed on the screen. 2. The notification message must be a privacy and/or security policy statement that is consistent with applicable federal regulations and privacy laws. |
| Part c | **Public Accessibility**  For public accessibility of the information system such as websites, the system must be configured to ensure that it:   1. Displays system use notification before granting further access. 2. Displays references to monitoring, recording, or auditing that are consistent with privacy and security laws for systems that prohibit specific activities like disclosure of government information. 3. Includes a description of the authorized uses of the system. That is the notice given to public users of the information system must describe authorized uses of the system. |

### AC-10 Concurrent Session Control (M) (H)

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

| AC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Administrators, Developers | |
| Parameter AC-10-1: system accounts and any other privileged account types | |
| Parameter AC-10-2: 1 | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-10 What is the solution and how is it implemented? |
| --- |
| The System Owner and the ISSO must coordinate to establish the required concurrent session limit for system accounts and any other privileged account types. Selection of the specific thresholds should be based on the account type (such as privileged user, non-privileged user, domain, or specific application) as well as the system or information that is being accessed. Implementation of Concurrent Session Control To prevent attackers from creating a denial of service situation by consuming all available sessions; the information system should be configured to create new sessions and invalidate the previous sessions when the session limits are exceeded.  There should be warning statements generated by the information system to prompt users when the new session has caused another session to be terminated.  The following parameters for implementation of concurrent session control must be followed to support system security.   * 1. Applications must prevent users from establishing simultaneous sessions unless there is a business need to support multiple sessions per user.  The business need should be documented and communicated to the ISSO and SO for approval.   2. Applications must provide a function for users to view and terminate any active sessions.   3. If multiple sessions are permitted, activity on one session cannot reset the idle timeout on other sessions.   4. Applications should notify a user when they logon of any other currently active sessions. |

### AC-11 Session Lock (M) (H)

The information system:

1. Prevents further access to the system by initiating a session lock after [fifteen (15) minutes] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AC-11(a): Prevents further access to system by initiating session lock after fifteen minutes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user |
| Part b | Retains the session lock until the user reestablishes access using established identification and authentication procedures |

#### AC-11 (1) Control Enhancement (M) (H)

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

| AC-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
| The session lock control enhancement requires that information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. |

### AC-12 Session Termination (M) (H)

The information system automatically terminates a user session after [certain conditions or triggered events requiring such termination].

| AC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AC-12: Session termination/User-initiated logouts/Message display | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-12 What is the solution and how is it implemented? |
| --- |
| Enforcement of this security control requires that the information system automatically terminates a user-initiated logical sessions when the following conditions or triggered events are detected:   1. User initiates the logout process. This can be done via the 'Logout' button or in the MAX Desktop application upon completion of the Citrix Sign-Out process. 2. Violation of the concurrency requirement of an application. Applications are expected to determine if it is appropriate to allow simultaneous logins from various sources for a single user. If this action by policy of the application is detected and not in compliance with the requirements of said application, then all user sessions must be terminated. 3. Violation of the application idle user policy. Applications are required to identify what is an acceptable timeout (inactivity, total session, etc) for all user sessions based on the requirements of the application. Any user session that is outside of this timeout should be terminated, and the user required to re-authenticate in order to establish a new session. |

### AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

1. 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
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner and ISSO | |
| Parameter AC-14(a): Permitted actions without identification or authentication | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Proper identification and authentication of the user is needed before system actions are allowed. |
| Part b | Exceptions to the policy must be granted by the System Owner and approved by the ISSO |

### AC-17 Remote Access (L) (M) (H)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner and ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Remote access approval:  Remote access shall be approved by the System Owner and the ISSO prior to implementation. Approval should be granted only after it is demonstrated that the remote access method provides for secure transfer of information in both directions, that authentication and authorization rules are enforced, and that a business need to allow remote access exists.  Privileged users accessing information systems remotely will use approved remote access methods using a two-factor authentication. It is the system owner’s responsibility to establish and document system access restrictions based on assessment of risk and to eventually allow remote access if appropriate.  Remote access methods with the highest degree of isolation should be preferred. For example, allowing remote access over a citrix or other VDI platform is preferable to allowing a direct connection over a VPN. |
| Part b | Secure remote access:  The system must be configured to allow authorized and necessary users access to the system. Specific requirements should be determined based on the role of the user and the level of access being granted. In all case The system must be set up to use encrypt technology to protect information between the remote user and the information system. Encrypt technology include (SSL/TLS, Secure Shell, and IPsec).  For normal interactions with web applications no additional mitigations may be required.  For direct access to information systems where users may be able to execute arbitrary commands against the operating system or database, additional steps should be taken to mitigate risk.   1. Remote sessions must be accessed through a limited number of managed access control points. Access control points may include secure VPN connections as well as access through specialized web applications. For example, access to internal resources may be available to users outside the information system boundary through a Citrix server that requires 2 factor authentication. 2. The information system must employ automated mechanisms to monitor and control remote access methods. |

#### AC-17 (1) Control Enhancement (M) (H)

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System, ISSO and System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
| Employing automated mechanisms to monitor and control remote access. |

#### AC-17 (2) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

| AC-17 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
| System is to be configured to allow authorized users to access the system while protecting the confidentiality of the information system. System must be configured using encryption technology to protect information between the remote user(s) and the information system. System administrators need to ensure encryption is compliant with Federal Information Security Management (FISMA). |

#### AC-17 (3) Control Enhancement (M) (H)

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

| AC-17 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-17(3): Must traverse a managed network access control point designed to enforce remote access restrictions before connecting to a target destination | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
| All remote access connections must traverse a managed network access control point designed to enforce remote access restrictions before connecting to a target destination. The access control point should reduce the possible attacks to the system. At a minimum, keep vulnerabilities at the lowest by incorporating the concept of Trusted Internet Connections (TIC) requirements for external network connections to the information system |

#### AC-17 (4) Control Enhancement (M) (H)

The organization:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and
2. Documents the rationale for such access in the security plan for the information system.

| AC-17 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter AC-17(4)(a): execution of privileged commands and access to security relevant information via remote access is authorized only for compelling operational needs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Must have documentation which states the rationale for access in the security plan of the system |
| Part b | System Owner and ISSO will ensure the conditions which allow for the system to be accessed remotely are met and documented in the system security plan. |

#### AC-17 (9) Control Enhancement (M) (H)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [FedRAMP Assignment: fifteen (15) minutes].

| AC-17 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AC-17(9): Speed of disconnect must be determined by the ISSO based on the criticality of the information system’s mission. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
| Firewalls must be set to detect unauthorized access. System administrator must be alerted when the firewalls detect unauthorized access. |

### AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Wireless access is not permitted within the information system. |
| Part b | Wireless access is not permitted within the information system. |

#### AC-18 (1) Control Enhancement (M) (H)

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

| AC-18 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter AC-18 (1): N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
| Wireless access is not permitted within the information system. |

### AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Mobile Devices are not permitted within the information system. |
| Part b | Mobile Devices are not permitted within the information system. |

#### AC-19 (5) Control Enhancement (M) (H)

The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

| AC-19 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter AC-19(5)-1: N/A | |
| Parameter AC-19(5)-2: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-19 (5) What is the solution and how is it implemented? |
| --- |
| Mobile Devices are not permitted within the information system. |

### AC-20 Use of External Information Systems (L) (M) (H)

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:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing official and System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Access the information system from outside the information system boundary. |
| Part b | Process, store, or transmit organization-controlled information using the external Information system. |

#### AC-20 (1) Control Enhancement (M) (H)

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:

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

| AC-20 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization imposes limits on the use of external information system unless implementation of the required security control are verified as outlined in the system security plan. |
| Part b | The system connection and processing agreements must be retained and frequently updated by the host of the external information system. |

#### AC-20 (2) Control Enhancement (M) (H)

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

| AC-20 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AC-20(2): Prohibit use of organization controlled portable storage devices in external information systems | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
| The use of non-organization-controlled portable storage devices in external information systems is strictly prohibited.  Under no circumstances should a portable storage device form an external information system be connected to the internal information system directly. |

### AC-21 Information Sharing (M) (H)

The organization:

1. 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
2. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

| AC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter AC-21(a):N/A | |
| Parameter AC-21(b): N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | MAX.gov prohibits the storage of privileged medical information, personally identifiable information, and classified information. |
| Part b | MAX.gov prohibits the storage of privileged medical information, personally identifiable information, and classified information. |

### AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [FedRAMP Assignment: at least quarterly] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AC-22: at least quarterly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All information within the Information System Boundary shall require successful user authentication with the following exceptions:   1. The MAX.gov login and user registration pages require unauthenticated access to perform their core functions. The content of these pages should be updated only through the approved Configuration Management process. 2. The MAX Survey application allows the creation of anonymous and unauthenticated surveys. A MAX.gov staff member must coordinate with the user to be sure they understand the risks and issues associated with an anonymous and unauthenticated survey. |
| Part b | 1. The CM Board is trained to identify any non-public information during the change review process. 2. Survey administrators are counseled prior to the setup of an anonymous survey to prevent disclosure of non-public information. |
| Part c | 1. The CM Board reviews al change to publicly accessible content on MAX.gov sites. 2. Survey administrators are counseled to review changes to anonymous survey content to prevent disclosure of non-public information. |
| Part d | A review must be conducted at least quarterly to check the contents of publicly accessible information. Any nonpublic information found on the publicly accessible information system during review must be removed immediately. |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
2. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
4. Reviews and updates the current:
5. Audit and accountability policy [FedRAMP Assignment: at every 3 years]; and
6. Audit and accountability procedures [FedRAMP Assignment: at least annually].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Assurance Team (IAT) | |
| Parameter AU-1(a): Develops, documents and disseminates to information system users | |
| Parameter AU-1(b)(1): every calendar year | |
| Parameter AU-1(b)(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization ensures that AU policy is reviewed and updated every calendar year. However, there may be an update to the document when there is a change in any of the control implementation, or when there is a change to the system’s control requirements. Changes to the document must be documented, dated and signed in accordance with NIST and FedRAMP guidance for retaining document history. |
| Part b | Audit and accountability policy must be reviewed and updated as needed at least every three years. Audit and accountability procedures must be reviewed and updated every year. |

### AU-2 Audit Events (L) (M) (H)

The organization:

1. Determines that the information system is capable of auditing the following events: [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes];
2. 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;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 to be audited continually for each identified event].

AU-2 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

| AU-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, ISSO and Authorizing Official | |
| Parameter AU-2(a): Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data and changes | |
| Parameter AU-2(d): All events identified in AU-2(a) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system’s capability to record all auditable events shall be reviewed as part of the configuration management process. Auditing of events shall be a critical design requirement and shall be included early in the SDLC.  Auditable events must be monitored continuously and in real time. Specific system or application audit settings may be noted in the system security plan and should themselves be monitored and any change captured for auditing.  Information system auditable events may be determined based on current threat information and an ongoing assessment of system risk. The determination of what events are to be audited within the information system and the frequency of each audit may change over time. Changes in the list of auditable events will be communicated to the system owner and implementation of new auditing requirements will be tracked.  The current auditable events for all systems are:   1. account management events 2. successful and unsuccessful account logon events 3. object access 4. policy change 5. privileged functions 6. process tracking 7. system events   For all web applications as well as Splunk, Zabbix, CAS, Tenable Nessus, BigFix, HP Web Inspect, and RSA Archer, the following audit events are also required:   1. all administrator activity, 2. authentication checks, 3. authorization checks, 4. data deletions, 5. data access, 6. data changes |
| Part b | The System Owner in coordination with the ISSO and the Information Assurance Team (IAT) may coordinate with the security audit function of other organizational entities such as service providers requiring audit-related information. This will provide support and help in selecting the appropriate auditable events for the information system. Coordination between service provider and the organization shall be documented and accepted by the Authorizing Official. |
| Part c | At least annually the auditable events should be reviewed by the System Owner and the ISSO and a memo prepared for the Authorizing Official documenting that the auditable events are appropriate and sufficient to support after the fact forensic analysis of security incidents. The memo should be stored along with other artifacts showing continuous monitoring. |
| Part d | All events identified in AU-2(a) must be monitored for all information system components. |

#### AU-2 (3) Control Enhancement (M) (H)

The organization reviews and updates the audited events [annually or whenever there is a change in the threat environment].

AU-2 (3) Additional FedRAMP Requirements and Guidance:

Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

| AU-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner and ISSO | |
| Parameter AU-2(3): annually or whenever there is a change in the threat environment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
| At least annually, the auditable events must be reviewed by the System Owner and the ISSO and a memo prepared for the Authorizing Official documenting that the auditable events are appropriate and sufficient to support the forensic analysis of security incidents. The memo should be stored along with other artifacts showing continuous monitoring.  Auditable events must also be reviewed by the ISSO when the organization is notified of a new threat. |

### AU-3 Content of Audit Records (L) (M) (H)

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.

| AU-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| 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.  The requirements for the content and format of audit records is found on the MAX Logging Standards community page (https://community.max.gov/x/EQqPIw). |

#### AU-3 (1) Control Enhancement (M)

The information system generates audit records containing the following additional information: [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].

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines audit record types [FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]. The audit record types are approved and accepted by the JAB.

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

| AU-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AU-3(1): session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
| The information system audit records must also contain, when applicable:   * session, connection, transaction, and activity duration; * for client-server transactions, the number of bytes received and bytes sent; * additional informational messages to diagnose or identify the event; * characteristics that describe or identify the object or resource being acted upon. |

### AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

| AU-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AU-4: allocates audit record storage capacity in accordance with | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| Implementation of this control involves a consideration of the types of auditing to be performed and the auditing processing requirements when allocating audit storage capacity based on the auditable list described in AU-2 policy.  The information system must be configured to allocate sufficient storage capacity for the systems audit logs. FedRAMP provides the minimum required standards on audit storage capacity as follows:   * If audit logs are archived on a daily basis, then it is recommended that triple the size of the current daily log file should be free to hold the audit logs. * If the audit logs are archived on a weekly basis, then it is recommended that 10 times the size of the current daily log file should be free to hold the audit logs. * If the audit logs are not archived, except on a monthly basis or longer. Then it is recommended that a server is dedicated to generating and storing said audit records. * The system owner (SO) in coordination with the ISSO must establish the appropriate storage capacity for the information system to ensure allocation of audit record storage and configuration to reduce the likelihood of exceeding the capacity limits. |

### AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

1. Alerts [MAX System Administrators and MAX Information Assurance Team] in the event of an audit processing failure; and
2. Takes the following additional actions: [critical system level logging data is written to its own reserved space, disabling logging processes required at the highest level of privilege on the system, highly restricting writing permissions on the log partition, conducting application logs like Catlina.out or the rail logs not stored in the same log partition].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: MAX.gov systems | |
| Parameter AU-5(a): Alerts MAX System Administrators in the event of an audit processing failure | |
| Parameter AU-5(b): continue to operate | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Failure of any audit process must alert the System Administrators and Information Assurance Team. Audit processes must be monitored in real time by both host based and external processes. |
| Part b | In the event of an audit process failing, [the](http://max.gov/) information systems may be permitted to continue to operate. The organization must take extensive steps to mitigate this risk by reducing the possible scenarios which would result in the log process failing:   * Critical system level logging data is written to its own reserved space (Windows log or a separate log partition for Linux) so processes that fill all available disk space should not impact the disk space available for logging. * Disabling logging processes requires the highest level of privilege on the system. * Write permissions on the log partition are highly restricted, preventing an attacker from using captured or legitimately issued credentials to fill the log partition and perform undetected actions that would normally be logged by system processes like auditd or sudo. * Application logs like Catalina.out or the rails logs are not stored in the same log partition. These are in the same partition as the application so if the disk fills up, in addition to logging failing the app is probably going to fail because the disk is full and most apps don’t like that. |

### AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

1. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
2. Reports findings to [Assignment: organization-defined personnel or roles].

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the Authorizing Official. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

| AU-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization’s designated personnel or management | |
| Parameter AU-6(a)-1: daily | |
| Parameter AU-6(a)-2: excessive failures, unauthorized changes, other Indicators of Compromise | |
| Parameter AU-6(b): Information Assurance Team and System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Audit logs must be reviewed by the organization’s designated personnel or management. Reviews must be performed daily on normal business days to identify any unusual activity within the information system. |
| Part b | The Information Assurance team will determine if the incident should be reported to the United States Computer Emergency Readiness Team (US-CERT) or if coordination with any other law enforcement entity is required for further investigations and actions.  The System owner is responsible for ensuring that data owners and other potentially impacted users are notified of any incidents. |

#### AU-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| AU-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
| All auditable information must be automatically collected into a log aggregation and analysis system such as Splunk or Kibana. The aggregated data must be made available to support audit review, analysis, and reporting processes while still being restricted based on least-privilege requirements. |

#### AU-6 (3) Control Enhancement (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
| All auditable information must be automatically collected into a log aggregation and analysis system such as Splunk or Kibana. The aggregated data must be made available to support audit review, analysis, and reporting processes while still being restricted based on least-privilege requirements. |

### AU-7 Audit Reduction and Report Generation (M) (H)

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

| AU-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system must be configured to:  * Support on demand audit review, analysis, and reporting requirements including after-the-fact investigations of security incidents: and Prevent alteration of the original content or time ordering of audit records.  Support of Audit Review, Analysis, and Reporting Requirements The information system must generate a reporting data store of audit records to support evidence collection for the investigations of security incidents without altering original audit records. This may include filtering raw audit records for events of interest based on selectable criteria, transferring audit records to alternative formats that are easier to review such as loading text log files into a database, or reformatting log entries to facilitate consumption by humans or other processes. In all cases, the original audit record in its entirety must be preserved and any summary records must clearly identify the original record.  Audit reduction refers specifically to processes using tools and techniques that reduce audit data in order to save storage space. This can include actions such as data compression of original records, deduplication of records recorded in multiple logs, abstracting more useful, higher-level data for the review process, or filtering of extraneous information. In all cases, the original audit record in its entirety must be preserved and any summary records must clearly identify the original record. Compliance The system owner in coordination with the ISSO must ensure audit records are available to the information assurance team in a way that allows flexible and timely analysis to support real time data driven decision making in response to emerging threats. |
| Part b | The information system must generate a reporting data store of audit records to support evidence collection for the investigations of security incidents without altering original audit records. In all cases, the original audit record in its entirety must be preserved and any summary records must clearly identify the original record. |

#### AU-7 (1) Control Enhancement (M) (H)

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

| AU-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AU-7(1): all auditable fields | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-7 (1) What is the solution and how is it implemented? |
| --- |
| A robust and dynamic search capability must be provided to allow authorized users to find relevant audit records quickly and easily. |

### AU-8 Time Stamps (L) (M) (H)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [integrated with records from other systems].

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AU-8(b): integrated with records from other systems | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Owner in coordination with the ISSO must ensure the information system uses internal system clocks to generate time stamps for audit records.  Time stamps generated by the information system include both date, time, and an indicator of time zone. Time stamps should be recorded at least to the millisecond level. |
| Part b | This level of information assures that all records can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and integrated with records from other systems. |

#### AU-8 (1) Control Enhancement (M) (H)

The information system:

1. Compares the internal information system clocks with [authoritative Network Time Protocol server] [at least hourly]]; and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

AU-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: The service provider selects primary and secondary time servers used by the NIST Internet time service, or by a Stratum-1 time server. The secondary server is selected from a different geographic region than the primary server.

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server. Synchronization of system clocks improves the accuracy of log analysis.

| AU-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AU-8(1)(a)-1: authoritative Network Time Protocol server | |
| Parameter AU-8(1)(a)-2: at boot time and at least hourly | |
| Parameter AU-8(1)(b): 1 second | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system must be configured to synchronize internal information system clock automatically with an authoritative Network Time Protocol (NTP) server. |
| Part b | If a time difference greater than 1 second is detected, the system must update its clock to match the NTP server. |

### AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| Audit information includes audit records, audit settings, and audit reports needed to successfully audit information system activity. Audit information must be protected end to end including protection in transit, in process, and at rest. |

#### AU-9 (2) Control Enhancement (M) (H)

The information system backs up audit records [nightly] onto a physically different system or system component than the system or component being audited.

| AU-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter AU-9(2): nightly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
| The information system must be configured to enable back up of audit records onto a separate system. Audit records must be backed up at least nightly. |

#### AU-9 (4) Control Enhancement (M) (H)

The organization authorizes access to management of audit functionality to only [senior members of the Information Assurance Team and the Lead System Architect for the Information System].

| AU-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AU-9(4): senior members of the Information Assurance Team and the Lead System Architect for the Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
| Administrative access which would allow a user to modify settings or to edit/delete a record in log aggregations system shall be granted only to senior members of the Information Assurance Team (such as the ISSO, ISSM, and Chief Security Architect) and the Lead System Architect for the Information System. |

### AU-11 Audit Record Retention (M)

The organization retains audit records for [ninety (90) days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter AU-11: until it is determined that they no longer needed for administrative, legal, audit or other operational purposes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. |

### AU-12 Audit Generation (L) (M) (H)

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [all information system is capable of generating audit records];
2. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System and (personnel) | |
| Parameter AU-12(a): all information system components which are capable of generating audit records | |
| Parameter AU-12(b): System Architects and the ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All information systems shall be evaluated as part of the configuration management process to confirm that the system generates audit records for the events defined in AU-2a with the content defined in AU-3. |
| Part b | The system Architect in coordination with the ISSO may determine that particular elements of a required auditable event are collected on another component in the information system. In this case the specific element need not be logged on other components for that event. |
| Part c | All information systems shall be evaluated as part of the configuration management process to confirm that the system generates audit records for the events defined in AU-2d with the content defined in AU-3. |

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
2. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
4. Reviews and updates the current:
5. Security awareness and training policy [FedRAMP Assignment: at least every 3 years]; and
6. Security awareness and training procedures [FedRAMP Assignment: at least annually].

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-1(a): All internal system users | |
| Parameter AT-1(b)(1): at least every 3 years | |
| Parameter AT-1(b)(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The policy is developed based on federal directives, guidelines, Executive orders, OMB circulations/memorandum and regulations. The system owner in coordination with the ISSO must approve the policy and procedure document before dissemination. After an approval is obtained, the policy and procedure document must be disseminated and circulated to information system users. |
| Part b | This policy must be reviewed and updated annually .There must also be an update to the document when there is a change in any of the AT Family control implementations, or when there is a change to the policy. Changes to the document must be dated and signed in accordance with NIST guidance. |

### AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AT-2(c): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Users of the information system must receive security awareness training. Training of system users must include managers, senior executives, and contractors. The training must be conducted to address specific needs as follows:   * + As part of initial training for new users   + When required by information system changes; and   + The frequency of refresher training as determined by the organization or the system owner.   **Initial Training for New Users**  Newly hired employees and contractors must receive appropriate training based on their roles and responsibilities. They must be aware of the policies and procedures that pertain to acceptable system use.  For non-privileged users, reading and acknowledging the rules of behavior must be sufficient.  For privileged users, the information system should enforce completion of training by new users prior to granting access. If a technical process is not feasible, system administrators must require confirmation that a user has completed training requirements prior to providing privileged access.  **Training Required by System Changes**  As part of the configuration management process the ISSO shall determine if additional security awareness training is required as a result of a system change. Training may be required for all users or only for users with a specific role. The ISSO shall also determine if training will be required before the change can be implemented. In this case, users who are unable to attend training shall have their access suspended until they are able to receive the updated training. The ISSO shall also determine if the training must be communicated to users through email, phone, and/or in-person training.  **Documentation of Training:**  For non-privileged users, the acceptance of the Rules of Behavior must be captured and retained as evidence of compliance with this policy.  For privileged users, the user’s attendance/completion of training along with a copy of the training materials must be retained by the Information Assurance team.  **Exceptions to Policy**  The System owner in coordination with the ISSO shall provide any exceptions to this policy. Exceptions may be granted to address short term critical business needs or to facilitate the smooth operation of the organization.  **Important Consideration: Security Awareness Training Content**  The ISSO must ensure that the information system’s security awareness training reflects the organization’s security requirements, policies and procedures. It must address the specific system(s) to which a user will have authorized access. Security awareness training content must include an explanation of the need to protect the security posture of the information system, specific guidance on security best practices, and information about other critical system policies and procedures related to information security.  Displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events are techniques which may be used to implement this control. |
| Part b | As part of the configuration management process the ISSO shall determine if additional security awareness training is required as a result of a system change. |
| Part c | Information system users with privileged access receive refresher training at least annually. |

#### AT-2 (2) Control Enhancement (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| AT-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-2 (2) What is the solution and how is it implemented? |
| --- |
| Security awareness training sessions must educate the system users about insider threats including how to recognize and report any indicators of insider threats. |

### AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner and ISSO | |
| Parameter AT-3(c): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | In addition to the training requirements specified in AT-3, users with privileged roles must receive additional training specific to their role(s) before authorizing access to the information system or performing assigned duties.   * All users of the information system and hosted information systems must be exposed to security awareness materials, at minimum, annually. System users include employees, contractors, visitors, and others who may need access to information systems and applications * Executives must receive training in information security basics and policy level in security planning and management * Program and functional managers must receive training in information security basics, management and implementation level training in security planning and system/application security management, and management and implementation level training in system/application life cycle management, risk management, and contingency planning * Chief Information Officers (CIO), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning * IT function management and operations personnel must receive training in information security basics, management and implementation level training in security planning and system/application security management, and management and implementation level training in system/application life cycle management, risk management, and contingency planning |
| Part b | In addition to the training requirements specified in AT-3, users with privileged roles must receive additional training specific to their role(s) when required by information system changes. The ISSO shall determine if additional training is required as part of the CM process and shall also determine if such training must be completed prior to deployment of the change, or within a specific time period after the change. The ISSO shall determine an acceptable time period and what actions must be taken if training is not completed including removing users from impacted roles. |
| Part c | All specified role based training must be included in annual refresher training sessions for users with those roles. |

### AT-4 Security Training Records (L) (M)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [FedRAMP Assignment: at least one year].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner and ISSO | |
| Parameter AT-4(b): at least one years | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Documentation of security training includes training records of basic security awareness training (as described in [AT-2](https://community.max.gov/x/wYp1W)) and specific role-based information system security training (as described in [AT-3](https://community.max.gov/x/wYp1W)).  The ISSO shall review training records at least annually to verify all privileged users have completed all required training. |
| Part b | Retention of security training records depends on the criticality of the particular system. The FedRAMP requirement for retaining security training records is one year. However, records may be retained for more years, depending on the sensitivity and criticality of the user’s system. |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
2. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
4. Reviews and updates the current:
5. Configuration management policy [every one (1) year]; and
6. Configuration management procedures [FedRAMP Assignment: at least annually].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-1(a): information system users | |
| Parameter CM-1(b)(1): every one year | |
| Parameter CM-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The current Configuration Management policy is made available through the Security Policy Portal |
| Part b | The Configuration Management policy is reviewed as part of the annual security assessment process and is updated as needed. |

### CM-2 Baseline Configuration (L) (M) (H)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| A baseline configuration is a well-defined, documented, and approved specification to which an information system is built. It describes the approved configuration of an information system including all its hardware, software, and firmware components; how the components are interconnected; and the physical and logical locations of each. The baseline configuration of an information system may evolve over time depending on the stage of the System Development Life Cycle (SDLC).  The baseline configuration must provide information about the components of an information system. These include the standard software load for each component including the operating system and any installed applications. The Baseline configuration must include the current version numbers and patch information for all software. The baseline must also describe the network topology and the logical placement of the components within the system architecture.  **Maintaining the baseline configuration:**  The current state of the system must match the current baseline plus any implemented changes. The baseline must be updated as needed to incorporate deployed changes so that the current system state is easy to determine and understand.  All configuration settings for information system components must be documented. This documentation must be sufficiently detailed to allow an experienced operator to recreate and redeploy the system from scratch. Any configuration setting which is not explicitly documented MUST be left in its default state. All configuration settings must reflect the most restrictive mode consistent with operational requirements. Baseline configurations should be established based on the latest NIST guidance and any deviation from NIST standards must be documented including the purpose/justification. |

#### CM-2 (1) Control Enhancement (M)

The organization reviews and updates the baseline configuration of the information system:

1. [yearly];
2. When required due to [a significant change happening within the information system]; and
3. As an integral part of information system component installations and upgrades.

| CM-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-2(1)(a): yearly | |
| Parameter CM-2(1)(b): a significant change occurs within the information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | At least once per year the information system baseline shall be reviewed for accuracy and all implemented changes merged into the baseline. |
| Part b | When a significant change occurs within the information system a new baseline shall be established. The new change -as well as all other implemented changes- shall be merged into the new baseline. |
| Part c | Whenever an information system component is installed or upgraded, a new baseline shall be established which includes the new component or reflects the new version information for an upgrade. Other pending changes shall also be incorporated into the baseline at this time. |

#### CM-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

| CM-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (2) What is the solution and how is it implemented? |
| --- |
| The baseline image may consist of the output of multiple processes. Where possible, the organization should favor automated options for maintaining the baseline. Examples include automatic inventory systems, network discovery tools, and Continuous integration/automated deployment tools. |

#### CM-2 (3) Control Enhancement (M)

The organization retains [organizational baseline configurations of the information system] to support rollback.

| CM-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-2(3): organizational baseline configurations of the information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
| The organization must retain prior versions of baseline configurations to support rollback. Baseline configurations must be maintained for hardware, software, firmware, and configuration files.  Information system components are required to develop and maintain rollback solutions for all changes. The duration for which rollback options must remain viable is determined by the Change Management Board |

#### CM-2 (7) Control Enhancement (M) (H)

The organization:

1. Issues [information systems, system components, devices notebook computers or mobile devices] with [additional security controls] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [specified safeguards] to the devices when the individuals return.

| CM-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter CM-2(7)(a)-1: N/A | |
| Parameter CM-2(7)(a)-2: N/A | |
| Parameter CM-2(7)(b): N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Anytime an information system component is removed from the secure data center it must be accompanied at all times by a responsible agent approved by the ISSO. The agent is responsible for ensuring that the information system is not altered or accessed while in transit. Other additional security measures may be required by the ISSO anytime an information system or component is removed from a secure facility. |
| Part b | When an information system component is returned to a secure data center it can be treated as secure if the stipulations in Part a have been followed. If the system was outside the control of the responsible agent for any period of time it should be considered compromised and must be inspected before being connected to the information system. Specific procedures for inspection and if necessary sanitization shall be determined by the ISSO. |

### CM-3 Configuration Change Control (M) (H)

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];

CM-3 (e) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with record retention policies and procedures.

1. Audits and reviews activities associated with configuration-controlled changes to the information system; and
2. Coordinates and provides oversight for configuration change control activities through [FedRAMP Assignment: see additional FedRAMP requirements and guidance] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

CM-3 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-3(e): In accordance with record retention policies and procedures | |
| Parameter CM-3(g)-1: the Configuration Management Board | |
| Parameter CM-3(g)-2: at least twice weekly | |
| Parameter CM-3(g)-3: if change requests have been submitted | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All changes to the information system are subject to configuration control once deployed into the production environment. |
| Part b | Changes must be reviewed and approved in compliance with the Configuration Management Procedure. The Configuration Management Procedure must explicitly include consideration for security impact of the change. |
| Part c | The Change Management procedure must also ensures that change approval is documented, implementation of the change is recorded, and that records of the change are available until deemed no longer necessary by the System owner in accordance with record retention policies and procedures. |
| Part d | Approved change requests must include the scheduled time for deployment of the change. If the change is not deployed as planned the change request must be updated and, at the Change Manager’s discretion, may need to be re-approved by the Change Management Board. |
| Part e | Records of all change must be maintained until deemed no longer necessary by the System owner in accordance with record retention policies and procedures. |
| Part f | The information assurance team will routinely verify deployed configurations by comparing them to the Configuration Baseline including any approved changes. |
| Part g | The Change Management procedure is maintained by the Configuration Management Board which must consist at a minimum of representatives from the Development, Technology Services, Data Management and Information Assurance teams. The Configuration Management Procedure must allow for rapid deployment of changes to meet the business needs of the information system. |

#### CM-3(2)  TEST / VALIDATE / DOCUMENT CHANGES

**The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.**

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All Change Requests must contain a detailed description of the configurations settings being deployed as well as a specific process for verifying settings are correctly applied post deployment. Change Requests must include a back out strategy to reverse a change if needed. Change Requests must identify any other dependencies of the change so that the initial state of the information system can be validated prior to deployment and so that dependent changes are rolled back along with any change they depended on.  Deviations and Exceptions  Critical changes may be deployed prior to compliance with this policy with the approval of the CMB Lead, the [MAX.gov](http://max.gov/) Policy lead, the Technology Services Team lead of the [MAX.gov](http://max.gov/) ISSO.  Recognizing the [MAX.gov](http://max.gov/) supports many critical and time sensitive missions across the federal government, If a Change Requestor is unable to reach any of the emergency change approvers, the Change Requester should use his or her best judgment.  The MAX ISSO and MAX Information Assurance team must be notified of any critical changes being deployed in this manner before deployment.  Once the change is deployed, the Change Requestor must immediately complete a CRF for the change and submit it to the CMB Lead for expedited review.  Any issues with the change must be addressed immediately.  Configuration changes made through an automated process or information system that has been reviewed and approved for the purpose of making that change do not require a separate Change Request unless:   * The change requires coordination between multiple system components, or * The change requires an update to the System Security Plan including changes to System Configuration Baseline(s), Security Policies, Security procedures, or Security diagrams such as the Data Flow or Authorization Boundary diagrams |

### CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

| CM-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-4 What is the solution and how is it implemented? |
| --- |
| Changes must be reviewed and approved in compliance with the Configuration Management Procedure. The Configuration Management Procedure must explicitly require consideration for security impact of the change. |

### CM-5 Access Restrictions for Change (M) (H)

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

| CM-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 What is the solution and how is it implemented? |
| --- |
| All changes must be documented and reviewed through the configuration management process which includes documentation of the specific person(s) who will deploy the change. Only authorized personnel shall be permitted to deploy changes to the information system.  Deployments involving the addition or removal of physical hardware must also be approved and overseen by the Network Administration Lead.  Deployment of new software or changes in configuration may be deployed by a system administrator, network administrator, database administrator, or by a senior developer.  In all cases deployment of changes must include coordination with the Technology Services Lead and the ISSO. |

#### CM-5 (1) Control Enhancement (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| CM-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
| All information system components shall maintain access logs as well as automated logging of changes to system configuration or deployment of new software that is under change control.  The information system’s ISSO and/or management personnel must audit information system changes weekly to determine whether unauthorized changes have occurred. |

#### CM-5 (3) Control Enhancement (M) (H)

The information system prevents the installation of [software and hardware] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CM-5 (3) Additional FedRAMP Requirements and Guidance:

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| CM-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter CM-5(3): software and firmware components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
| Before installing any software and firmware version updates, patches, service packs, device drivers, and Basic Input Output System (BIOS) updates the user implementing the change must verify that the update is signed with a valid, trusted digital signature/certificate OR; If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) must be used.  Integrity checks should be automated when possible and should prevent the installation if integrity cannot be verified. |

#### CM-5 (5) Control Enhancement (M) (H)

The organization:

1. Limits privileges to change information system components and system-related information within a production or operational environment; and
2. Reviews and reevaluates privileges [weekly].

| CM-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-5(5)(b): weekly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Privileges to change information system components and system-related information within a production or operational environment must be limited to only those individuals who possess both the necessary training AND have an operational need to possess such privileges. If a user requires these privileges only at specific times (i.e. when a new software version is approved for deployment) permissions must be granted as needed and revoked promptly once necessary work is completed. |
| Part b | Current privileges to change information system components and system-related information within a production or operational environment shall be reviewed and reevaluated weekly. |

### CM-6 Configuration Settings (L) (M) (H)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance] that reflect the most restrictive mode consistent with operational requirements;

CM-6(a) Additional FedRAMP Requirements and Guidance:

Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (<http://scap.nist.gov/>) validated or SCAP compatible (if validated checklists are not available).

Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>.

1. Implements the configuration settings;
2. Identifies, documents, and approves any deviations from established configuration settings for [information systems] based on [operational requirements]; and
3. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-6(a)-1: Center for Internet Security guidelines (Level 1) to establish configuration settings or the organizational developed secure configuration baselines (approved by the Chief Information Officer (CIO), Chief Information Security Officer (CISO) or designees)that reflect the most restrictive mode consistent with operational requirements are established and documented | |
| Parameter CM-6(a)-2: | |
| Parameter CM-6(c)-1: information system components | |
| Parameter CM-6(c)-2: approved operational requirements | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Baseline configuration settings for all information system components shall be derived from Center for Internet Security guidelines (Level 1) or the organizational developed secure configuration baselines (approved by the Chief Information Officer (CIO), Chief Information Security Officer (CISO) or designees)that reflect the most restrictive mode consistent with operational requirements which are established and documented. |
| Part b | Information System components shall be configured in compliance with the approved baseline configuration settings. |
| Part c | Exceptions, based on explicit operational requirements, from the baseline configuration settings for individual components within the information system must be explicitly identified and documented as a change request. The change request must include the details of the alternative configuration, the business justification for the change and any additional mitigations implemented to reduce the risk posed by the exception. These exceptions must be approved by the ISSO and the SO. |
| Part d | Information System Components shall be regularly reviewed for compliance with the expected configuration and any deviation shall be recorded, investigated and resolved by either changing the setting to comply with the approved configuration or creating a change request as outlined in Part c. |

#### CM-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [the information system’s Local Area Network (LAN)].

| CM-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-6(1): information system’s Local Area Network (LAN) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
| The information system must employ automated mechanisms that centrally manage, apply, and verify configuration settings of components on the information system. The information system must employ automated mechanisms (e.g. McAfee File Integrity checker) to respond to unauthorized changes to authorization systems; system configurations, log files, and critical system files (including sensitive system and application executable, libraries, and configurations). |

### CM-7 Least Functionality (L) (M) (H)

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services [United States Government Configuration Baseline (USGCB)]

CM-7 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-7(b): United States Government Configuration Baseline (USGCB) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization shall review the information system and eliminate all unnecessary functions of the system. Where feasible, the organization must limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems or individual components of information systems, must be carefully reviewed to determine which functions and services are candidates for elimination.  Unused physical ports, logical ports, protocols (e.g., Universal Serial Bus (USB), File Transfer Protocol (FTP), etc.) on information system components are restricted to prevent unauthorized device connections, unauthorized information transferring, or unauthorized tunneling  Network scanning tools, intrusion detection and prevention systems, and end-point protections (e.g., firewalls and host-based intrusion detection systems) should be used to identify and prevent the use of prohibited functions, ports, protocols, and services |
| Part b | The information system shall specifically prohibit or restrict functions, ports, protocols, and/or services identified in the Center for Internet Security guidelines (Level 1). If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and document a justification statement as to how they came up with the baseline configuration settings.  Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline> |

#### CM-7 (1) Control Enhancement (M) (H)

The organization:

1. Reviews the information system [monthly] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].

| CM-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-7(1)(a): monthly | |
| Parameter CM-7(1)(b): organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must regularly scan the information system for open ports or operating services that are not approved. The organization must also monitor for the use of unapproved protocols. |
| Part b | Default system configurations must disable functions, ports, protocol, and services deemed to be unnecessary and/or non-secure. A specific list of blacklisted functions, ports, and protocols must be maintained and systems must be scanned for any usage of blacklisted elements. |

#### CM-7 (2) Control Enhancement (M) (H)

The information system prevents program execution in accordance with [Selection (more): [organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

CM-7 (2) Additional FedRAMP Requirements and Guidance:

Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e., white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

| CM-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter CM-7(2): whitelisting | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
| The organization must maintain a list of whitelisted software and must prevent any software not specifically included in the whitelist from executing on information system components. |

#### CM-7 (5) Control Enhancement (M)

The organization:

1. Identifies [organizational software programs authorized to execute on the information system];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [annually].

| CM-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-7(5)(a): organizational software programs authorized to execute on the information system | |
| Parameter CM-7(5)(c): annually and as part of the Configuration Management Process | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must maintain a list of whitelisted software. |
| Part b | The organization must prevent any software not specifically included in the whitelist from executing on information system components. |
| Part c | The whitelisted software must be reviewed at least annually to identify and eliminate any programs that are no longer needed. The software whitelist must also be updated as part of the Change Management Process if an approved change will require new software to execute on information system components. |

### CM-8 Information System Component Inventory (L) (M) (H)

The organization:

1. Develops and documents an inventory of information system components that:
2. Accurately reflects the current information system;
3. Includes all components within the authorization boundary of the information system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes [hardware inventory specifications, software license information, information system/component owner, the component network name and network address]; and
6. Reviews and updates the information system component inventory [FedRAMP Assignment: at least monthly].

CM-8 Additional FedRAMP Requirements and Guidance:

Requirement: Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-8(a)(4): hardware inventory specifications, software license information, information system/component owner, the component network name and network address | |
| Parameter CM-8(b): at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Organization must ensure an inventory of information system components is developed, documented, and maintained which:   * 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 where applicable:   + - Hardware inventory specifications (manufacturer, type, model, serial number, and physical location);     - Software license information;     - Information system/component owner;     - Component network name;   Network address;   * Is available for review and audit by designated organizational officials.   The Organization must ensure that all components within the authorization boundary of the information system are either inventoried as a part of the system, or recognized and verified by another system as a component within that system. The inventory of information system components must be updated as an integral part of component installations, removals, and information system updates. |
| Part b | Inventory information must be validated at least monthly. This validation may be through an automated process which compares inventory entries to actual assets detected using network discovery tools. An automated process should not automatically correct the inventory system to match the discovered assets. Inconsistencies in the inventory database must be flagged and manually investigated. |

#### CM-8 (1) Control Enhancement (M) (H)

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| CM-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (1) What is the solution and how is it implemented? |
| --- |
| Updates, additions, and deletions form the inventory system must be an explicit checklist item for all change requests. |

#### CM-8 (3) Control Enhancement (M) (H)

The organization:

1. Employs automated mechanisms [FedRAMP Assignment: Continuously, using automated mechanisms with a maximum five-minute delay in detection] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Takes the following actions when unauthorized components are detected: [Selection (more): disables network access by such components; isolates the components; notifies [agency- defined personnel or roles]].

| CM-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-8(3)(a): Continuously, using automated mechanisms with a maximum five-minute delay in detection | |
| Parameter CM-8(3)(b): disables network access for such components; isolates the components; notifies agency-defined personnel | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system. |
| Part b | The automated process must take the following actions when unauthorized components are detected:   * Disable network access for such components * Isolate the components * Notify the agency-defined personnel   + Configuration Manager   + Information Security Office (ISO)   + MAX Information Assurance Team Member (IAT) |

#### CM-8 (5) Control Enhancement (M) (H)

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

| CM-8 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
| The organization shall maintain a comprehensive system inventory for all information systems. This inventory must have a specific field for specifying the authorization boundary in which an inventory entity is included. An entity may only be included in one (1) authorization boundary. |

### CM-9 Configuration Management Plan (M) (H)

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan for unauthorized disclosure and modification.

| CM-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The configuration management plan satisfies the requirements in the organization’s configuration management policy, while being tailored to a specific information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support life-cycle development activities at the information system level.  The plan must describe the following:   * How to move a change through the change management process * How configuration settings and configuration baselines are updated after a change is implemented * How to maintain the information system component inventory * How development, test, and operational environments are controlled * How documents are developed, released, and updated. |
| Part b | Items must be placed under configuration control once released into the production environment. Development teams are encouraged to implement their own configuration control processes during earlier phases of the SDLC. |
| Part c | The configuration management plan must clearly describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and how documents are developed, released, and updated. |
| Part d | The configuration management plan shall be itself managed through the configuration management process including protecting the configuration management plan from unauthorized disclosure and modification. |

### CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

| CM-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Technology Services Team Lead is responsible for ensuring that the organization is in compliance with all contract agreements and copyright laws in regards to software used within the information system. All new software acquisition, including procurement as well as usage for free or open source software, must be reviewed by the Information Assurance team. The IA team is responsible for ensuring that the technology services team lead is aware of the applicable laws and restrictions. The IA team may include the organization General Counsel to consult. New software acquisition may not proceed until approved by the ISSO and the System Owner. |
| Part b | The Technology Services Lead shall maintain a record of all software in use within the information system including number and type of licenses and how those licenses are assigned, if applicable, within the information system. |
| Part c | Peer-to-peer file sharing technology shall not be used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. |

#### CM-10 (1) Control Enhancement (M) (H)

The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions]

| CM-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-10(1): Open Source software must be approved and managed in the same manner as commercial software. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-10 (1) What is the solution and how is it implemented? |
| --- |
| Open Source or otherwise no-cost software must be managed in the same manner and with all the same restrictions as other software as described in CM-10 |

### CM-11 User-Installed Software (M) (H)

The organization:

1. Establishes [policies] governing the installation of software by users;
2. Enforces software installation policies through [automated methods, if feasible]; and
3. Monitors policy compliance [quarterly, at a minimum].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CM-11(a): policies | |
| Parameter CM-11(b): automated methods, if feasible | |
| Parameter CM-11(c): quarterly, at a minimum | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Deployment of new software may be conducted only by a system administrator. Deployment of new software must include coordination with the Technology Services Lead and the ISSO.  Other users of the information system may be permitted to install software in sandboxed environments created by the technology services team and approved for such use by the Information Assurance team. Sandboxed environments may be destroyed and recreated at any time without notice so it is critical that users maintain explicit records and deployment scripts to recreate their working environments. Sandbox environments must be isolated form the information system production components and are considered outside the security boundary. Any connection between a sandboxed environment and the information system shall be documented in a System Interconnection Agreement. |
| Part b | Software installation policies shall be enforced through restricted permissions and application whitelisting. |
| Part c | In addition to tightly restricting the permissions to install new software, the information system shall continuously scan for installed software and compare it against a database of approved software. Any installed software found on the information system that is not on the approved list shall be immediately deactivated and a security incident created. |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
2. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
4. Reviews and updates the current:
5. Contingency planning policy [FedRAMP Assignment: at least every one (1) year].; and
6. Contingency planning procedures [FedRAMP Assignment: at least annually].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-1(a): information system users | |
| Parameter CP-1(b)(1): at least every one year | |
| Parameter CP-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | After an approval is obtained, the policy and procedure document must be disseminated to information system users. |
| Part b | The organization ensures that CP policy is reviewed and updated at least once a year. |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
2. Identifies essential missions and business functions and associated contingency requirements;
3. Provides recovery objectives, restoration priorities, and metrics;
4. Addresses contingency roles, responsibilities, assigned individuals with contact information;
5. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
6. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
7. Is reviewed and approved by [designated officials within the agency];
8. Distributes copies of the contingency plan to [relevant system owners and stakeholders];
9. Coordinates contingency planning activities with incident handling activities;
10. Reviews the contingency plan for the information system [annually];
11. 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;
12. Communicates contingency plan changes to [the CIO]; and
13. Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-2(a)(6): The System Owner and the ISSO | |
| Parameter CP-2(b): internal users and other interested stakeholders | |
| Parameter CP-2(d): annually | |
| Parameter CP-2(f): internal users and other interested stakeholders | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must develop and document a contingency plan to provide critical services in the event of a wide range of disruptions. The contingency plan must identify essential mission and business functions and associated contingency requirements to provide essential services.  The contingency plan must include recovery objectives, restoration priorities, and metrics. Objectives and priorities should be determined analyzing the impact of a service or function being unavailable, degraded, or otherwise compromised. The plan must specify contingency roles, responsibilities, and list assigned individuals including contact information.  The contingency plan must provide assurance that maintaining essential missions and business functions despite an information system disruption, compromise, or failure is assured within a reasonable level of certainty. The System Owner and the ISSO are responsible for reviewing the Contingency Plan to ensure that it meets this criterion.  The contingency plan must also addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented. |
| Part b | The contingency plan must be distrusted to all individuals assigned a role within the plan. It should also be distributed to internal users and other interested stakeholders with appropriate redactions to support least-privilege protection of any sensitive information. |
| Part c | The organization must coordinate contingency plan development with organizational elements responsible for related plans for contingency operations and incident response. Contingency plans for the organization may include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation, and Occupant Emergency Plans.  It is vital that the various contingency and incident response plans do not interfere with or delay each other activities. |
| Part d | The contingency plan must be reviewed at least annually. |
| Part e | The contingency plan must be updated and reviewed whenever changes to the organization, information system, or environment of operation change. Changes in assigned individuals do not require a review of the entire plan.  If problems are encountered during contingency plan implementation, execution, or testing the contingency plan must be updated as part of an after action review process. |
| Part f | When updated, the contingency plan must be distrusted to all individuals assigned a role within the plan. It should also be distributed to internal users and other interested stakeholders with appropriate redactions to support least-privilege protection of any sensitive information. |
| Part g | The organization must protect the contingency plan from unauthorized disclosure and modification. The Contingency Plan must be managed through the organizations CM process. The organization is also encouraged to label any sensitive information in the plan so it can be easily redacted when the plan is shared. |

#### CP-2 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (1) What is the solution and how is it implemented? |
| --- |
| The organization must coordinate contingency plan development with organizational elements responsible for related plans for contingency operations and incident response. Contingency plans for the organization may include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation, and Occupant Emergency Plans.  It is vital that the various contingency and incident response plans do not interfere with or delay each other activities. |

#### CP-2 (2) Control Enhancement (M) (H)

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

| CP-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (2) What is the solution and how is it implemented? |
| --- |
| The organization must conduct quarterly capacity planning assessments to verify that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.  This should be performed as part of a quarterly Contingency plan test. |

#### CP-2 (3) Control Enhancement (M) (H)

The organization plans for the resumption of essential missions and business functions [immediately within the period of contingency plan activation.

| CP-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-2(3): as soon as possible | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
| The contingency plan must also addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented. Full information system restoration must be pursued as soon as possible. |

#### CP-2 (8) Control Enhancement (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

| CP-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
| The organization must identify critical information system assets which support essential missions and business functions. These assets should be designated in the system inventory as critical and listed in the Contingency Plan. The list must be exhaustive but contain only those assets truly critical to supporting essential missions and business functions. |

### CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [FedRAMP Assignment: ten (10) days] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [annually] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-3(a): 10 days of assuming a contingency role or responsibility | |
| Parameter CP-3(c): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-3 What is the solution and how is it implemented? |
| --- |
| The organization shall develop a contingency plan training program which familiarizes participants with the Contingency Plan. This training shall be provided annual and all individuals with an assigned role must attend.  Additionally, any time a new individual is assigned a role in the contingency plan, the ISSO or a designee shall provide specific one-on-one training within 10 days to ensure the new individual understands their role and responsibilities and is prepared to carry out assigned tasks. This includes verifying that the individual has the required authorizations, skills and knowledge.  The ISSO may require any individual to attend additional contingency plan training as needed in response to information system changes or contingency plan test results. |

### CP-4 Contingency Plan Testing (M)

The organization:

1. 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;

CP-4(a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-4(a)-1: at least semi-annually, following organizational or system changes, or  the issuance of new TT&E guidance, or as otherwise needed | |
| Parameter CP-4(a)-2: approved test plans developed in accordance with NIST SP 800-34 and conducted in as close to an operational environment as possible | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must conduct planned tests of the Contingency Plan at least twice a year. Organizational or system changes, the issuance of new TT&E guidance, or other special circumstances may require additional tests. The need for additional testing in response to change is determined as part of the Change Management process. Other instances were additional testing is needed are determined by the ISSO.  Tests must use quantifiable metrics to validate the operability of the information system or system component in an operational environment. For example, an organization could test call tree lists to determine if calling can be executed within prescribed time limits; another test may be removing power from a system or system component. Tests must be conducted in as close to an operational environment as possible; if feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used.  The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an ISCP.  Executing contingency plans during controlled tests and/or exercises provide a mechanism to test the effectiveness of the CP,  The organization must ensure to perform tests and/or implement the system’s contingency plan (CP) annually using defined tests and exercises, such as the tabletop test, to determine the plan's effectiveness and organizational readiness to execute the plan. |
| Part b | The organization must document all activities during the Contingency Plan test. A scribe should be assigned to record activity and communication during the test. A report of the test including results, deficiencies, and suggested corrective actions must be developed and delivered to the ISSO, System Owner, and other stakeholders within 3 business days of the conclusion of the test. |
| Part c | The organization must review the CP test results, provide training, and correct weaknesses in the plan, and initiate reasonable and appropriate corrective actions to close or reduce the impact of CP failures and deficiencies. Any deficiencies that cannot be corrected within timelines provided in RA-5 shall be documented in the POAM. |

#### CP-4 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| CP-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
| The organization shall coordinate contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity, Disaster Recovery, Incident Response, Continuation of Operations Plan) or impacted services. The date, time, and scope of any test must be communicated to the organization to prevent or minimize disruption to other activities. If a portion of a planned test overlaps with portions of other related plans it is recommended that the relevant portion of related plans be included in the test to most closely mimic a realistic scenario. |

### CP-6 Alternate Storage Site (M) (H)

The organization:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

| CP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization requires that an alternate storage site be maintained at all times. The alternate site must be capable of storing all information system data for an indefinite period of time including all prior versions of data that are required under organizational policies or procedures.  The alternate storage site must allow for retrieval of stored data at any time. The organization must determine the maximum time required to recover data from the alternative storage site if data at the primary site is lost. |
| Part b | The alternate storage site must provide information security safeguards that are comparable to the protections of the primary storage site, or provide compensating controls that can meet this requirement. |

#### CP-6 (1) Control Enhancement (M) (H)

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

| CP-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
| The alternate storage site must be geographically separated (at least 50 miles) from the primary storage site, so it will not be susceptible to the same hazards as the primary site.  The System Owner in coordination with the ISSO must determine what is considered as a sufficient degree of separation between the primary and alternate storage sites (the 50 mile requirement is the minimum) based on the types of threats that are of concern. The alternate site must be approved by the Authorizing Official. |

#### CP-6 (3) Control Enhancement (M) (H)

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.

| CP-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
| The organization must identify and provide solutions to any potential access problems that affect the alternate storage site. Potential access problems may be due to large scale disasters such as a hurricane, earthquake, or regional power outage. The organizational risk assessments must account for site accessibility issues and identify mitigations. |

### CP-7 Alternate Processing Site (M) (H)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [information system operations] for essential missions/business functions within [Recovery Time Objective (RTO)] when the primary processing capabilities are unavailable;

CP-7a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. 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
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-7(a)-1: all information system operations | |
| Parameter CP-7(a)-2: Recovery Time Objectives | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization requires that an alternate processing site be maintained at all times. This may be the same or different than the alternate storage site. The alternate site must be capable of processing all information system functions for an indefinite period of time at the same level of service as the primary site.  The alternate processing site may be a hot, warm, or cold site but must be capable of assuming primary processing responsibility within organization defined Recovery Time Objectives.  Recovery Time Objectives shall be established for each information system component as part of the initial deployment. Recovery Time Objectives must be documented in the Contingency Plan. |
| Part b | The organization must confirm equipment and supplies required to resume operations within the specified Recovery Time Objectives (RTO) are available at the alternate site or contracts are in place to deliver to the site in time to support the organization-defined RTOs. Availability of equipment and supplies should be verified during initial deployment and during Contingency Plan Testing. |
| Part c | The alternate processing site must provide information security safeguards that are comparable to the protections of the primary site, or provide compensating controls that can meet this requirement. |

#### CP-7 (1) Control Enhancement (M) (H)

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (1) Additional FedRAMP Requirements and Guidance

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites will be less relevant.

| CP-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
| The alternate processing site must be geographically separated (at least 50 miles) from the primary site, so it will not be susceptible to the same hazards as the primary site.  The System Owner in coordination with the ISSO must determine what is considered as a sufficient degree of separation between the primary and alternate sites (the 50 mile requirement is the minimum) based on the types of threats that are of concern. The alternate site must be approved by the Authorizing Official. |

#### CP-7 (2) Control Enhancement (M) (H)

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.

| CP-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
| The organization must identify and provide solutions to any potential access problems that affect the alternate processing site. Potential access problems may be due to large scale disasters such as a hurricane, earthquake, or regional power outage. The organizational risk assessments must account for site accessibility issues and identify mitigations. |

#### CP-7 (3) Control Enhancement (M) (H)

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

| CP-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
| Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site. All external agreements necessary to provide alternative processing services must include relevant Recovery Time Objectives which must be agreed to by the provider. |

### CP-8 Telecommunications Services (M) (H)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [information system operations] for essential missions and business functions within [12 hours of] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

| CP-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-8-1: informational system operations | |
| Parameter CP-8-2: 12 hours | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 What is the solution and how is it implemented? |
| --- |
| The organization must ensure establishment of alternate telecommunication services and the necessary agreements needed to permit the resumption of information system operations for essential missions and business functions, within 12 hours in the event that the primary telecommunication capabilities become unavailable.  The System Owner in coordination with the ISSO must determine what is considered as a sufficient degree of separation between the primary and alternate telecommunication services based on the types of threats that are of concern. The alternate telecommunication services must be approved by the Authorizing Official. |

#### CP-8 (1) Control Enhancement (M) (H)

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. 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.

| CP-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site. All external agreements necessary to provide alternative telecommunication services must include relevant Recovery Time Objectives which must be agreed to by the provider. |
| Part b | In the event that the primary and/or alternate services are provided by a common carrier, Telecommunication Service Priority should be requested for telecommunication services used for national security emergency preparedness. |

#### CP-8 (2) Control Enhancement (M) (H)

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

| CP-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
| Alternate telecommunication services should be selected so as to eliminate or reduce shared points of failure with the primary telecommunication services.  To the extent possible alternative telecommunication services should not rely on any component or service of the primary provider. |

### CP-9 Information System Backup (L) (M) (H)

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

1. Conducts backups of user-level information contained in the information system [weekly]

CP-9 (a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

1. Conducts backups of system-level information contained in the information system [weekly];

CP-9 (b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

1. Conducts backups of information system documentation including security-related documentation [annually or when there are major changes ]; and

CP-9 (c) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online).

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-9(a): weekly | |
| Parameter CP-9(b): weekly or when there are major changes | |
| Parameter CP-9(c): annually or when there are major changes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organizational must complete full back-ups weekly to separate media, and perform incremental or differential back-ups daily to separate media. Back-ups are to include user-level and system-level information (including system state information). |
| Part b | The organizational designated personnel must perform full back-ups weekly or when there are major changes to system level information to separate media, and perform incremental or differential back-ups daily to separate media. Back-ups are to include user-level and system-level information (including system state information). |
| Part c | Designated organizational personnel must also conduct backups of system documentation at least annually, or when there are major changes. |
| Part d | Back-up media must be encrypted to protect the confidentiality and integrity of the content, and stored at an appropriate secure location(s). |

#### CP-9 (1) Control Enhancement (M)

The organization tests backup information [monthly] to verify media reliability and information integrity.

| CP-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-9 (1): monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
| The information system must undergo monthly tests, for back-up information, to verify media reliability and information integrity. |

#### CP-9 (3) Control Enhancement (M) (H)

The organization stores backup copies of [critical information such as operating systems, cryptographic key management systems, and intrusion detection/prevention systems] in a separate facility or in a fire-rated container that is not collocated with the operational system.

| CP-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CP-9(3): critical information such as operating systems, cryptographic key management systems, and intrusion detection/prevention systems | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
| The organization must store back-ups of critical information system software, data, and configurations in a separate facility or in a fire-rated container that is not collocated with the operational system. Cloud storage solutions may be used for this purpose.  Critical software, data, and configurations shall be defined by the ISSO and may include, for example:   * Custom operating system installation media, * Software licenses and license keys, * cryptographic key management systems, and * intrusion detection /prevention system configurations |

### CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| The following are required for recovery and reconstitution:   * Secure information system recovery and reconstitute to the system’s original state which entails:   + All system parameters (either default or established by the system) are reset   + Patches are reinstalled   + Configuration settings are reestablished   + System documentation and operating procedures are available   + Application and system software are reinstalled   + Information from the most recent back-ups are available   + The system is fully tested * Recovery and reconstitution mechanisms must be documented in the contingency plan * If a system is transaction-based, the information system must implement transaction recovery (e.g., transaction rollback and transaction journaling) as specified in the contingency plan * Provide compensating security controls for circumstances that inhibit recovery * Reconstitute to a known state * Provide the capability to reimage information system components and support target recovery times through configuration-controlled and integrity-protected disk images that are representing a secure, operational state for the components |

#### CP-10 (2) Control Enhancement (M) (H)

The information system implements transaction recovery for systems that are transaction-based.

| CP-10 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
| The SO in coordination with the ISSO must ensure the implementation of transaction recovery for transaction-based systems. |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
2. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
4. Reviews and updates the current:
5. Identification and authentication policy [FedRAMP Assignment: at least every one (1) year]; and
6. Identification and authentication procedures [FedRAMP Assignment: at least annually].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-1(a): information system users | |
| Parameter IA-1(a): at least every one year | |
| Parameter IA-1(b)(1): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | After an approval is obtained, the policy and procedure document must be disseminated to information system users. |
| Part b | The organization ensures that IA policy is reviewed and updated every one year. |

### IA-2 User Identification and Authentication (L) (M) (H)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

| IA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 What is the solution and how is it implemented? |
| --- |
| All information system functions, with the exception of user authentication, must require that the user or process is authenticated using an account issued exclusively to that user or process. Two kinds of accounts are permitted within the information system. User accounts which are issued to a specific user and service accounts issued for a specific process. Credentials for user accounts must never be shared. Credentials for service accounts may be shared if required for troubleshooting or operational maintenance but must only be used to support the specific process for which the account was issued. Shared accounts are not permitted and anonymous access to functions other than authentication is not permitted unless specifically approved by the System Owner and ISSO.  For additional details on Account Policies, see policy AC-2.  User identity must be verified each time a user access a protected function to determine if the user has been properly authenticated and if the user possesses the correct authorizations to perform the requested function. The ability of a user or process to send a request must NEVER be used as a means of authentication or indentification. |

#### IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| Access to privileged accounts is permitted only from the PITC and OMB Private Cloud networks. Users must authenticate using a valid PIV, CAC, or equivalent credential to access these networks. This ensures that access to privileged accounts always requires multi-factor authentication.  The accounts used to access the PITC and OMB Private Cloud networks are non-privileged. Users with access to privileged accounts then connect to a specific host with a privileged account or use SUDO or similar functions to execute commands with a privileged account. When possible the second level authentication must also use MFA. |

#### IA-2 (2) Control Enhancement (M) (H)

The information system implements multifactor authentication for network access to non-privileged accounts.

| IA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (2) What is the solution and how is it implemented? |
| --- |
| The information system supports multi-factor authentication for all user accounts. At the discretion of the System Owner, non-privileged users may be permitted to connect using single factor authentication to support necessary business functionality. |

#### IA-2 (3) Control Enhancement (M) (H)

The information system implements multifactor authentication for local access to privileged accounts.

| IA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (3) What is the solution and how is it implemented? |
| --- |
| Access to privileged accounts is permitted only from the PITC and OMB Private Cloud networks. Users must authenticate using a valid PIV, CAC, or equivalent credential to access these networks. This ensures that access to privileged accounts always requires multi-factor authentication.  The accounts used to access the PITC and OMB Private Cloud networks are non-privileged. Users with access to privileged accounts then connect to a specific host with a privileged account or use SUDO or similar functions to execute commands with a privileged account. When possible the second level authentication must also use MFA. |

#### IA-2 (5) Control Enhancement (M) (H)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

| IA-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (5) What is the solution and how is it implemented? |
| --- |
| The use of shared accounts within the information system is not permitted. In the event that multiple privileged users requires the ability to run commands as a service account, the users must FIRST authenticate using an individual account before being permitted to execute a command as the service account. |

#### IA-2 (8) Control Enhancement (M) (H)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (8) What is the solution and how is it implemented? |
| --- |
| Network access to privileged accounts is permitted only over an encrypted connection to prevent an attacker from capturing the authentication handshake. When possible authentication must use a secure authentication framework such as Active Directory or LDAP which include protections against replay attacks. |

#### IA-2 (11) Control Enhancement (M) (H)

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 [FedRAMP Assignment: FIPS 140-2, NIAP\* Certification, or NSA approval].

\*National Information Assurance Partnership (NIAP)

Additional FedRAMP Requirements and Guidance:

Guidance: PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).

| IA-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter IA-2(11): FIPS 140-2, NIAP\* Certification, or NSA approval | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (11) What is the solution and how is it implemented? |
| --- |
| MFA for remote access to privileged accounts must require PIV or equivalent as one factor in the authentication process. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.  Access to non-privileged accounts may use other MFA solutions such as [Time-based One-time Password Algorithm](https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm) (TOTP; specified in [RFC 6238](https://tools.ietf.org/html/rfc6238)) and [HMAC-based One-time Password algorithm](https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm) (HOTP; specified in [RFC 4226](https://tools.ietf.org/html/rfc4226)). |

#### IA-2 (12) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

IA-2 (12) Additional FedRAMP Requirements and Guidance:

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
| The information system must support Personal Identity Verification (PIV) and Common Access Card (CAC) credentials as a means of authentication. This includes verification of the integrity of the certificate chain and the revocation status of the credentials. |

### IA-3 Device Identification and Authentication (M) (H)

The information system uniquely identifies and authenticates [all devices] before establishing a [local, remote, or network] connection.

| IA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter IA-3-1: all devices | |
| Parameter IA-3-2: local network | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-3 What is the solution and how is it implemented? |
| --- |
| The information system identifies devices connected to the internal local network b IP address. Any device connecting to the local network must present an IP address specifically defined in the information system inventory. Any device presenting an IP address not defined in the inventory must be prevented form communicating with any other device on the local network.  Because of the use of IP address as a unique identifier, the information system security team must be extremely vigilant in monitoring for and responding to IP address conflicts or unexpected changes in ARP tables. |

### IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [System or Application Owners] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [one calendar year or longer based on the needs of the system]; and
5. Disabling the identifier after [120 days of inactivity)]

IA-4e Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP http://iase.disa.mil/cloud\_security/Pages/index.aspx.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-4(a): A Federal Agency or authorized information system user | |
| Parameter IA-4(d): the lifespan of the information system | |
| Parameter IA-4(e): after a period of inactivity determined, in part, based on the strength of the identifier and the sensitivity of the data or functions available. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Only users with a valid email account provided by an approved Federal agency or sponsored by a valid user with appropriate training and authority may be granted an account to access the information system. |
| Part b | A User’s account must be assigned a globally unique identifier such as an individual (not shared) email address, Active Directory account, or LDAP userID |
| Part c | Credentials for authenticating with the user’s account shall be distributed, if necessary, in a secure manner and in a separate communication from distribution of the account identifier. |
| Part d | The globally unique identifier assigned to an account shall not be re-used. In the event that a identifier must be re-used (e.g. an email address is re-used by an agency for a new person) the exception to this policy must be approved by the System Owner or the ISSO. |
| Part e | Account identifiers must be disabled after a period of inactivity. This period shall be determined, in part, based on the strength of the identifier and the sensitivity of the data or functions available. Identifier’s based on user created passwords shall be disabled after 90 days regardless of activity. PIV or CAC identifiers may remain valid for up to a year with no activity. |

#### IA-4 (4) Control Enhancement (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [contractors; foreign nationals].

| IA-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-4 (4): Federal or Non-Federal | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-4 (4) What is the solution and how is it implemented? |
| --- |
| A users account must clearly identify if they are a Federal Employee or not. Other information about the user such as contractor status should also be included if relevant. |

### IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

**IA-5 Additional FedRAMP Requirements and Guidance:**

**Requirement:** Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 2. Link <https://pages.nist.gov/800-63-3>.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-5(g): as needed to improve the strength of the authenticator type. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Authenticators such as digital certificates, passwords, and private keys must be distributed in a manner that provides the strongest possible assurance of the recipient Identity. This can best be accomplished by relying on an already strong authenticator such as a Federal Agency issued network credential or a PIV/CAC card.  Inspection of valid government issued ID is also an acceptable method of verifying a users identity. |
| Part b | Initial authenticator values should be left as null and the authenticator should be disabled until the user can set the authenticator’s value.  For service accounts, authenticator values should be randomly generated and must be of sufficient complexity to prevent compromise through brute force attacks. The authenticator value must be distributed only to the user responsible for the service account using an out of band communication channel different than the system for which the authenticator is to be used. |
| Part c | The ISSO shall review all acceptable authenticators used by the information system at least annually and make recommendations to the System Owner and Authorizing Official to retire any that do not provide a sufficient strength of mechanism for their intended use. |
| Part d | Initial authenticator values should be left as null and the authenticator should be disabled until the user can set the authenticator’s value.  For service accounts, authenticator values should be randomly generated and must be of sufficient complexity to prevent compromise through brute force attacks. The authenticator value must be distributed only to the user responsible for the service account using an out of band communication channel different than the system for which the authenticator is to be used. |
| Part e | When installing software to any component within the information system, the default content of all authenticators must be changed prior to allowing the software to be accessed by any user other than the installation team. Default authenticators must be changed even if the account they are associated with is not being used or is disabled. |
| Part f | User created authenticator values shall be restricted from re-use of the same value after a required update. System Owners shall determine if additional restrictions on re-use are required based on user behavior and the sensitivity of the system.  It is far better to educate users regarding bets practices for authenticator management and encourage the use of randomly generated authenticator values than to mandate reuse restrictions.  All service account passwords MUST be randomly generated and therefore should never be re-used. A specific randomly generated value should NEVER be used for more than one authenticator. |
| Part g | The organization shall require authenticator values to be changed when such requirements enhance the strength of the authenticator. Requiring users to change passwords too frequently results in poor security practices such as the use of patterns or storing passwords using insecure methods. The ISSO shall review the organizations password change policies as well as examining usage data regarding password changes and failed login attempts at least annually to determine if the current requirements for authenticator value changes are having the desired impact. |
| Part h | Authenticators shall be stored encrypted at all times using a strong one way hash and a SALT of sufficient complexity to inhibit the use of rainbow tables or other brute force attacks to determine the unencrypted value of the authenticator.  To ensure authenticator values are not changed by an unauthorized agent, all updates to the authenticator value shall require at least a two step process in which the user’s identity is confirmed. For example, if a user requests a password change the user should be sent a one use limited time link to their registered email. Accessing this unique link verifies the user requesting the password change has access to the registered email account. All request for changes and successful changes shall be logged in a reliable and secure fashion. |
| Part i | All users shall be required to keep their user authenticator values secret and may not share them with any other person.  Service account credentials must be protected using procedures specific to the purpose and sensitivity of the account. A specific procedure for managing authenticator values must be approved by the ISSO before a service account is created. |
| Part j | If a user with knowledge of a service account credential leaves the organization that credential must be changed within 24 hours. |

#### IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [case sensitive, minimum of eight (8) characters, at least one upper case letter, lower case letter, numbers and special character];
2. Enforces at least the following number of changed characters when new passwords are created: [at least one (1)];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [minimum one (1) day and maximum of ninety (90) days];
5. Prohibits password reuse for [twenty-four (24)] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

**IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:**

**Guidance:** If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter IA-5(1)(a): case sensitive, minimum of eight (8) characters, at least one upper case letter, lower case letter, numbers and special character | |
| Parameter IA-5(1)(b): at least one (1) | |
| Parameter IA-5(1)(d): minimum one (1) day and maximum of ninety (90) days | |
| Parameter IA-5(1)(e): twenty-four (24) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Passwords must be case sensitive, contain a minimum of eight (8) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters |
| Part b | At least one (1) character must be changed when a new password is created. For sensitive systems within the organization, at least fifty percent (50%) of the characters must be changed when a new password is created |
| Part c | The information system stores and transmits only cryptographically-protected passwords |
| Part d | The lifetime minimum must be one (1) day; the lifetime maximum must be ninety (90) days |
| Part e | Prohibits password reuse for at least twenty-four (24) generations |
| Part f | Allows the use of a temporary password for system logons with an immediate change to a permanent password |

#### IA-5 (2) Control Enhancement (M) (H)

The information system, for PKI-based authentication:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
2. Enforces authorized access to the corresponding private key;
3. Maps the authenticated identity to the account of the individual or group; and
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

| IA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information |
| Part b | Enforces authorized access to the corresponding private key |
| Part c | Maps the authenticated identity to the account of the individual or group |
| Part d | Maintains a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network |

#### IA-5 (3) Control Enhancement (M) (H)

The organization requires that the registration process to receive [system authenticators (Active Directory, LDAP, internal MAX.gov] be conducted [onsite (in person)] before [organization-defined registration authority] with authorization by [the Executive Office of the President].

| IA-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-5(3)-1: system authenticators (Active Directory, LDAP, internal MAX.gov) | |
| Parameter IA-5(3)-2: onsite (in person) | |
| Parameter IA-5(3)-3: System Owner or a designated representative | |
| Parameter IA-5(3)-4: the Executive Office of the President | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (3) What is the solution and how is it implemented? |
| --- |
| All users of the information system must first be issued credentials by an approved Federal Agency. This process is assumed to represent a sufficient validation of the user’s identity. The system owner may then determine the appropriate level of authorization to grant the user within the information system. |

#### IA-5 (4) Control Enhancement (M)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*control enhancements*].

IA-5 (4) Additional FedRAMP Requirements and Guidance:

Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators.

| IA-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-5(4): control enhancements | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (4) What is the solution and how is it implemented? |
| --- |
| Password complexity must be validated at the time the password is submitted to the information system to ensure it meets the requirements defined in IA-5(1). This validation must be performed within the information system boundary. This requirement may not be met by implementing validation in client or browser side code. |

#### IA-5 (6) Control Enhancement (M) (H)

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

| IA-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (6) What is the solution and how is it implemented? |
| --- |
| The organization must protect authenticators at the same or higher FISMA level as the highest rated system for which the authenticator may be used. Systems containing multiple security categories of information without reliable physical or logical separation between categories and authenticators used to grant access to the systems are protected with the highest security category of information on the systems. |

#### IA-5 (7) Control Enhancement (M) (H)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

| IA-5 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (7) What is the solution and how is it implemented? |
| --- |
| The organization requires that unencrypted static authenticators are not embedded in applications, access scripts, stored on function keys, or saved within configuration files. If there is no clear indication of whether the authenticator is encrypted or not, it is to be assumed that the authenticator is unencrypted and should not be stored. |

#### IA-5 (11) Control Enhancement (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [organizational requirements].

| IA-5 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Parameter IA-5(11): U.S. Government Personal Identity Verification (PIV) requirements | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
| The information system, for hardware token-based authentication, employs mechanisms that satisfy the U.S. Government Personal Identity Verification (PIV) for authentication. The system owner for specific and limited use may approve hardware tokens other than PIV. The System Owner and / or ISSO may define specific requirements for tokens, such as working with a particular PKI. |

### IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

| IA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-6 What is the solution and how is it implemented? |
| --- |
| To the extent possible the information system shall obscure the display of authenticator values in any interface where the user is required to prevent such values. Authenticator values shall not be saved in cookies, session variables, or any other mechanism nor shall the authenticator value be returned as part of an error message. This protects the information from possible exploitation or use by unauthorized individuals. |

### IA-7 Cryptographic Module Authentication (L) (M) (H)

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.

| IA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-7 What is the solution and how is it implemented? |
| --- |
| The information system employs mechanisms for authentication to a cryptographic module to authenticate and verify an operator accessing the module. This control requires that the information system implements mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. |

### IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

| IA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 What is the solution and how is it implemented? |
| --- |
| This control addresses identification and authentication requirements for non-organizational users. Non-organizational users include information system users other than organizational users explicitly covered by [IA-2](https://nvd.nist.gov/view/800-53/Rev4/control?controlName=IA-2). These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented within [AC-14](https://nvd.nist.gov/view/800-53/Rev4/control?controlName=AC-14). The information system ensures that non-organizational users who need access to the information system must comply with the E-Authentication E-Government initiative [policy](https://ieeexplore.ieee.org/abstract/document/7792024). The purpose of identification and authentication of non-organizational users is to protect federal, proprietary, or privacy-related information. The organization uses risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing these needs to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. |

#### IA-8 (1) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
| The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. |

#### IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
| The information system accepts only FICAM-approved third-party credentials. |

#### IA-8 (3) Control Enhancement (L) (M) (H)

The organization employs only FICAM-approved information system components in [information systems that are accessible to the general public] to accept third-party credentials.

| IA-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IA-8(3): information systems that are accessible to the general public | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
| The organization employs only FICAM-approved information system components to accept third-party credentials. This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Information System | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
| The information system conforms to FICAM-issued profiles. This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and Open ID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
2. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
4. Reviews and updates the current:
5. Incident response policy [annually]; and
6. Incident response procedures [annually].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-1(a): information system users | |
| Parameter IR-1(b)(1): annually | |
| Parameter IR-1(b)(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IR-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This policy requires that the SO in coordination with the ISSO must establish, maintain, and implement plans for emergency response, disaster recovery, back-up operations, and post-disaster recovery for their information systems. These should guarantee critical information resources are available and the continuation of operations in emergency situations. These plans must help the information system to recover from serious incidents involving it, and in minimum time and with minimum costs and disruption. The IR must be reviewed, updated, and tested annually to ensure its effectiveness.  Implementing this control involves having an information system’s IR policy and procedure. The policy and procedures are written in a manner that supports the effective implementation of selected security controls and control enhancements within the control family. The organization must develop, disseminate, review, and update the policies and procedures documents annually. The IR policies and procedures address the purpose, scope, roles, and responsibilities of selected security controls. Management commitment, coordination among organizational entities, and compliance with federal laws and regulations must be included.  **Develop, Document, and Disseminate Policy to Users**  The SO collaborates with the IAT to develop and document security policies and procedures on behalf of senior management. The policy is developed based on federal directives, National Institute of Standards and Technology (NIST) guidelines, executive orders, OMB circulations/memorandum, and regulations. The SO in coordination with the ISSO must approve the policies and procedures document before dissemination. After an approval is obtained, the policies and procedures document must be distributed to information system users. |
| Part b | **Policy Review and Update**  The organization ensures that the IR policy is reviewed and updated annually. However, there may be an update to the document when there is a change in any of the control implementations, or when there is a change to the system’s control requirements. Changes to the document must be documented, dated and signed in accordance with NIST and FedRAMP guidance for retaining document history. |

### IR-2 Incident Response Training (L) (M)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [a year] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [annually] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-2(a): a year | |
| Parameter IR-2(c): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Employees must be trained in their roles and responsibilities as they are stated in the incident response (IR) policies and procedures:   * Training must be provided to all users on how to report incidents, and to whom they should report them. * System users and managers shall be trained on how to identify and report incidents as part of the annual computer security awareness training. * IR personnel must undergo training relevant to their roles and responsibilities on how to handle and report an incident.   Incident response training includes training users on how to identify and report any suspicious activity, from both from external and internal sources:   * Offer training whenever there is a significant change in the information system environment or procedures, or when an employee enters a new position that requires additional role-specific training * Incorporate where possible simulated events into IR training to facilitate effective responses to prepare for a crisis situation(s) * Employ automated mechanisms to provide a more thorough and realistic training environment.   **The Chief Information Security Officer (CISO), Program Supervisors (PS) and Information System Security Officer (ISSO) must:**   * Train personnel in their incident response roles and responsibilities with respect to the information system * Provide annual refresher training   ISSOs must incorporate simulated events, by using automated mechanisms, into IR training to provide a more thorough and realistic training environment, as well as facilitate effective responses by personnel in crisis situations. |
| Part b | The organization must provide additional training whenever there is a significant change in the information system environment or procedures, or when an employee enters a new position that requires additional role-specific training |
| Part c | The organization must arrange annual refresher training for all internal users in their incident response roles and responsibilities with respect to the information system. |

### IR-3 Incident Response Testing (M)

The organization tests the incident response capability for the information system [annually] using [reviews, analysis, and simulations] to determine the incident response effectiveness and documents the results.

IR-3 Additional FedRAMP Requirements and Guidance:

Requirements: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). For JAB authorization, the service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to the test commencing.

| IR-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-3-1: annually | |
| Parameter IR-3-2: reviews, analysis, and simulations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-3 What is the solution and how is it implemented? |
| --- |
| **Roles and Responsibilities**   * Information Assurance Team (IAT) * System Owner (SO) * Information System Security Officer (ISSO) * System Administrator (SA) * Authorizing Official (AO) * Chief Information Security Officer (CISO)   **Control Requirements and Compliance**  The organization must prioritize how to respond to incidents based on functional impact, informational impact (confidentiality, integrity, and availability of the organizational information), and recoverability from the incident (time and resources). The organization must also annually test the Incident Response’s (IR) functionality using reviews, analysis, and simulations to determine the IR’s effectiveness and document the results. The following are standards set for IR testing:   * The IR’s functionality must be tested annually using scenario-based exercises to determine the ability of the personnel to respond to computer related security incidents * At a minimum, tabletop exercises must be performed; however, more robust exercises are recommended. * For information systems and their components containing sensitive information, the organization must coordinate with the federal partner to employ automated mechanisms to more thoroughly and effectively test the IR’s quality * The results of IR functionality testing must be used to identify and remediate potential weaknesses within the IR Plan * The appropriate personnel must review the IR test results, which must be documented in the IR plan, and initiate corrective actions * The organization will employ automated mechanisms to more thoroughly and effectively test their incident response capacity.   [NIST SP 800-61](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) provides sample scenarios for IR teams to use for a table top exercise. Tests and exercises must be performed in a controlled manner and the results must be analyzed, to determine the strengths and weaknesses of the organizational IR plan’s functionalities and how to improve on those functionalities.  **Frequency for System Testing**  The CISO, SO, and ISO should test the IR plan’s functionalities for the information system annually, using scenario based exercises to determine the IR plan’s effectiveness and document the results. The organization must employ automated mechanisms to more thoroughly and effectively test the incident response plan’s functionalities. |

#### IR-3 (2) Control Enhancement (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

| IR-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-3 (2) What is the solution and how is it implemented? |
| --- |
| IR testing may be more effective when coordinating the test plan with related system security plans such as the Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Critical Infrastructure Plans, and Occupant Emergency Plan. These system artifacts may provide additional information to support thorough IR testing. |

### IR-4 Incident Handling (L) (M) (H)

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

| IR-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The SO and ISSO must ensure:   * Incident handling functionalities for security incidents are implemented to include preparation, detection and analysis, containment, eradication, and recovery * Incident handling activities are coordinated with contingency planning activities * Lessons learned from ongoing incident handling activities must be incorporated into incident response procedures, training, and testing, as well as have the resulting changes implemented accordingly   Incident-related information can be obtained from a variety of sources including, but not limited to audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. In some cases attacks can happen throughout the organization that seem unrelated. The organization must employ automated mechanisms to support the incident handling process. This includes correlating information from individual incident responses to gain an organizational-wide perspective.  The organization must identify classes of incidents and ensure there is a responsive plan for each category. The response plan must ensure that the organizational mission and business functions are not interrupted. Response actions must be documented and kept in a secure repository.  The most recent cybersecurity counter measures must be used, a process for deploying those measures throughout the organization must be developed. |
| Part b | Since security incidents will often cause, or be caused by, other kinds of system disruptions the organization must include procedures to coordinate incident response activities with contingency planning activities. Contingency plans should, when possible, avoid altering or deleting forensic evidence that should be evaluated and preserved as part of the incident response. |
| Part c | Only qualified individuals should investigate incidents and conduct audits. Records of information security breaches and the remedies used to resolve them must be documented so they can become references for evaluating any future security breaches. The information must be logged and maintained in a location where the information cannot be altered by others. The recorded events must be analyzed and reviewed regularly to have as a reminder of the lessons learned. The lessons learned from incident handling activities must be incorporated into incident response procedures, training, testing, and the resulting changes must be implemented. This can eventually create processes to provide information to enhance the security of organizational information system security awareness programs and incident response programs. |

#### IR-4 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the incident handling process.

| IR-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| For timely and consistent handling of incidents, the organization must employ automated mechanisms to support the incident handling processes. It is essential for the information system to use automated processes to correlate security events with technologies such as Security Information and Event Management (SIEM). |

#### IR-4 (2) Control Enhancement (M) (H)

The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability.

| IR-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Technology Services | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| The organization includes dynamic reconfiguration as part of the incident response capability.  Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises.  Organizations include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats. |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-5 What is the solution and how is it implemented? |
| --- |
| The organization requires that security incidents are tracked and documented accurately. Records of security incidents must include the status of the incident, any pertinent information necessary for forensics during or after the incident, and metric categorization data used for evaluating incident trends and handling. |

### IR-6 Incident Reporting (L) (M) (H)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [one hour of discovery/detection]; and
2. Reports security incident information to [their manager and/or to the ISSO].

IR-6 Additional FedRAMP Requirements and Guidance

Requirement: Report security incident information according to FedRAMP Incident Communications Procedure.

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-6(a): one hour of discovery/detection | |
| Parameter IR-6(b): their manager and/or to the ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Users of federal information systems are required to report suspected security incidents to their manager and/or to the system’s point of contact within one hour of detecting suspicious activity. Contact information for reporting security incidents should be prominently displayed to users of the information system.  All system personnel and contractors must ***immediately*** *(no more than 30 minutes after becoming aware of the incident)*report suspected security incidents to the system’s point of contact. In addition, all systems personnel and contractors must promptly report any actual or suspected breaches of PII in accordance with the reporting procedures on the Privacy (PII) Web pages on the organizational intranet.  The timely reporting of incidents or suspected incidents assists with incident containment, impact, and mitigation. This includes reporting incidents dealing with Personally Identifiable Information (PII). A PII incident involves suspected and confirmed breaches in the protection of personally identifiable information in an electronic or physical form.  **Designated Incident Response Personnel must comply with the following steps when reporting a system incident:**   1. Identify the current level of impact on agency functions or services (functional impact) 2. Identify the type of information lost, compromised, or corrupted (information impact) 3. Estimate the scope of time and resources needed to recover from the incident (recoverability) 4. Identify when the activity was first detected and when corrective actions were implemented 5. Identify the number of impacted systems, records, and users 6. Identify the observed activity’s network location 7. Identify the point of contact’s information for additional follow-ups 8. Identify the attack vector(s) that led to the incident 9. The method of breach detection and incident response actions 10. Provide any indicators of compromise, including signatures or detection measures, developed in relationship to the incident 11. Provide any mitigation activities taken in response to the incident 12. If there are any supply chain aspects to the incident it must be reported to associated entities |
| Part b | Once an incident is reported, the ISSO in coordination with other stakeholders such as the system manager must review and document the incident and report it to the designated authority(s) within one hour of the incident occurring.  The ISSO should report the security incident information to designated authorities as directed by the Computer Security Incident Response Team (CSIRT).  The ISSO is responsible for reporting security incidents to the US-CERT within specified time frames, designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling, and if warranted to local or federal law enforcement. |

#### IR-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

| IR-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-6 (1) What is the solution and how is it implemented? |
| --- |
| The information system must employ automated mechanisms to assist in the timely reporting of security incidents. Network, host-based Intrusion Detection Systems (IDS) and other system monitoring tools can be utilized to provide automated detection of incidents and send alerts to appropriate security personnel. The organization may use automated tools to track and report possible security incidents, such as centralized service desk ticketing tools. |

### IR-7 Incident Response Assistance (L) (M) (H)

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.

| IR-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 What is the solution and how is it implemented? |
| --- |
| Organizational technical staff must provide incident response support resources as needed and organizational IT personnel, to offer advice and assistance to system users on how to handle and report security incidents.  A monitored email account or other active communication method shall be deployed to receive alerts from users of possible security incidents. |

#### IR-7 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 (1) What is the solution and how is it implemented? |
| --- |
| Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing the understanding of current response capabilities and support. |

#### IR-7 (2) Control Enhancement (M) (H)

The organization:

1. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
2. Identifies organizational incident response team members to the external providers.

| IR-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must establish a direct cooperative relationship between the incident response capabilities and external provider’s information system’s protection capabilities, as well as identify the external provider’s organizational incident response team members.  Incident response points of contact must be explicitly identified for all parties to any MOU, procurement, or ICA. |
| Part b | All MOUs or ICAs must explicitly define the communication channel for external entities to coordinate incident response activities with the organization. |

### IR-8 Incident Response Plan (L) (M) (H)

The organization:

1. Develops an incident response plan that:
2. Provides the organization with a roadmap for implementing its incident response capability;
3. Describes the structure and organization of the incident response capability;
4. Provides a high-level approach for how the incident response capability fits into the overall organization;
5. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
6. Defines reportable incidents;
7. Provides metrics for measuring the incident response capability within the organization;
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
9. Is reviewed and approved by [designated officials within the organization];
10. Distributes copies of the incident response plan to [CIO, SOs, ISOs and any additional staff as necessary].

IR-8(b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Reviews the incident response plan [annually];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [CIO, CISO, SO, ISSO and other impacted staff]; and

IR-8(e) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-8(a)(8): designated officials within the organization | |
| Parameter IR-8(b): CIO, SOs, ISOs and any additional staff as necessary | |
| Parameter IR-8(c): annually | |
| Parameter IR-8(e): CIO, CISO, SO, ISSO and other impacted staff | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | * Provides the organization with a roadmap for implementing its incident response capabilities * Describes the structure and organization of the incident response capabilities * Presents a high-level approach for how the incident response capability fits into the overall organization * Meets the unique requirements of the organization relating to its mission, size, structure, and functions * Defines reportable incidents within the information system * Provides metrics for measuring the incident response capability within the organization * Denotes the resources and management support needed to effectively establish and maintain incident response capabilities * Is reviewed and approved by designated officials within the organization |
| Part b | Distribute copies of the Incident Response Plan to the Chief Information Officer  (CIO), SOs, ISOs, and any additional staff as necessary |
| Part c | Review the Incident Response Plan, at the minimum, annually |
| Part d | Revise the Incident Response Plan to address system organizational changes or problems encountered during plan implementation, execution, or testing |
| Part e | Communicate Incident Response Plan changes to the CIO, CISO, SO, ISSO, and other impacted staff |
| Part f | Protect the Incident Response Plan from unauthorized disclosures and modifications |

### IR-9 Information Spillage Response (M) (H)

The organization responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [designated employees] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [organizational defined actions as specified in the incident response plan and procedures].

| IR-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-9(b): designated employees | |
| Parameter IR-9(f): organizational defined actions as specified in the incident response plan and procedures | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Identifying the specific information contaminated in the information system |
| Part b | Alerting designated employees of the information spill, using a method of communication not associated with the spill |
| Part c | Isolating the contaminated information system or system’s components |
| Part d | Eradicating the information from the contaminated information system or system’s component |
| Part e | Recognizing other information systems or system’s components that may have been subsequently contaminated |
| Part f | Performing other organizational defined action as specified in the incident response plan and procedures |

#### IR-9 (1) Control Enhancement (M) (H)

The organization assigns [designated personnel] with responsibility for responding to information spills.

| IR-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-9(1): designated personnel | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (1) What is the solution and how is it implemented? |
| --- |
| The SO must assign designated personnel the responsibility of responding to information spills. This will enable only approved organizational and qualified personnel to be in charge of the information spillage’s response. The organizational assigned personnel must be identified and documented. |

#### IR-9 (2) Control Enhancement (M)

The organization provides information spillage response training [frequently or least annually].

| IR-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-9(2) frequently or at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (2) What is the solution and how is it implemented? |
| --- |
| The organization must provide information spillage response training frequently, or a minimum, annually. The training requirements must be documented and followed accordingly. |

#### IR-9 (3) Control Enhancement (M) (H)

The organization implements [post-spill operations] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

| IR-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-9(3): post-spill operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (3) What is the solution and how is it implemented? |
| --- |
| The organization must implement post-spill operations to ensure that impacted personnel affected by information spills can continue to perform their assigned tasks, while contaminated systems are being recovered. Corrective actions for the information system, which is contaminated due to information spillage, may be very time-consuming and may potentially affect the organization’s ability to conduct organizational business. |

#### IR-9 (4) Control Enhancement (M) (H)

The organization employs [security safeguards] for personnel exposed to information not within assigned access authorizations.

| IR-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter IR-9(4): security safeguards | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (4) What is the solution and how is it implemented? |
| --- |
| The organization must employ security safeguards for personnel exposed to information who are not granted with access authorizations. Security safeguards include ensuring personnel exposed to spilled information become aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information. |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
   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
2. Reviews and updates the current:
   1. Media protection policy [every one (1) year]; and
   2. Media protection procedures [FedRAMP Assignment: at least annually].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-1(a): information system users | |
| Parameter MP-1(b)(1): every one (1) year | |
| Parameter MP-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | After an approval is obtained, the policies and procedures documents must be disseminated to information system users. |
| Part b | The organization ensures that MP policies are reviewed and updated every one year. |

### MP-2 Media Access (L) (M)

The organization restricts access to [secure sensitive information] to [store and present the information].

| MP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-2-1: sensitive information | |
| Parameter MP-2-2: only those users who require access for a specific business function | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-2 What is the solution and how is it implemented? |
| --- |
| Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.  In general, storage of sensitive information on removable storage media (including paper) should be avoided.  If storage of sensitive data on removable media is necessary, access controls including physical protection of, and accountability for, removable media must be enforced throughout the lifecycle of the media. Access controls must be designed to minimize the risk of damage or unauthorized changes to data stored on the removable storage media (Integrity) as well as theft of removable storage media or unauthorized access to data stored on the media (Confidentiality). If the data on the removable media is covered by any agreements with third parties the access controls must also prevent any software licensing violations.  Assessment of risk must guide the selection of media, and associated information contained on that media requiring restricted access. |

### MP-3 Media Labeling (M) (H)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [portable digital and non-digital media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

MP-3(b) Additional FedRAMP Requirements and Guidance:

Guidance: Second parameter in MP-3(b)-2 is not applicable.

| MP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-3(b)-1: portable digital and non-digital media intended for temporary storage less than 1 day | |
| Parameter MP-3(b)-2: the possession of a trusted internal user | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All removable media must be clearly marked indicating the distribution limitations, handling caveats, and any additional security requirements based on the information contained.  For digital media this shall be accomplished by placing the media in a sealed envelop and documenting the required information on the outside of the envelope. If possible, the information should also be documented on the media itself in both physical and digital means.  For non-digital media this information shall be included in document headers and footers printed on every page of the document as well as on a cover sheet prominently displayed.  If deemed necessary the media may be placed inside a second envelope or other container to mask its contents. |
| Part b | Temporary notes or digital media used to move data directly from one system to another with minimal delay may be exempted from these marking requirements. Such media must remain in the possession of a trusted user who has completed an SSBI investigation at all times and must be destroyed or sanitized using approved equipment, techniques, and procedures before the end of the user’s business day.  Any media that is being transferred from one user to another must be marked as described in Part a. |

### MP-4 Media Storage (M) (H)

The organization:

1. Physically controls and securely stores [digital and non-digital information system media] within [controlled areas using safeguards prescribed for the highest system security level of the information ever recorded on it]; and

MP-4a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

1. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

| MP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-4(a)-1: digital and non-digital media which contains sensitive information | |
| Parameter MP-4(a)-2: controlled areas using safeguards prescribed for the highest system security level of information ever recorded on it | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must protect digital and non-digital media which contains sensitive information in compliance with the highest security level ever required for the specific media. If the media is unmarked, the organization must protect the media at the highest security category for the information system until the media are reviewed and appropriately labeled.  Digital and non-digital media which contains sensitive information may be stored only in controlled areas such as a locked office or restricted access area. |
| Part b | The organization must protect digital and non-digital media which contains sensitive information until the media is destroyed or sanitized using approved equipment, techniques, and procedures. |

### MP-5 Media Transport (M) (H)

The organization:

1. Protects and controls [digital and non-digital containing sensitive information] during transport outside of controlled areas using [cryptography and tamper evident packing and had caring, or a securable container moved via authorized personnel if shipped, or tracked with receipt if moved with a commercial carrier];

MP-5a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

1. Maintains accountability for information system media during transport outside of controlled areas;
2. Documents activities associated with the transport of information system media; and
3. Restricts the activities associated with transport of information system media to authorized personnel.

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-5(a)-1: digital and non-digital media containing sensitive information | |
| Parameter MP-5(a)-2: cryptography and tamper evident packing, or a securable container moved via authorized personnel if shipped. If moved with a commercial carrier the shipment must be tracked with receipt and approved by the ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must protect and control digital and non-digital media containing sensitive information during transport outside of controlled areas using either:   * cryptography, * tamper evident packaging, * a securable container (e.g., locked briefcase) moved via authorized personnel if shipped, or * If moved with a commercial carrier the shipment must be tracked with receipt and approved by the ISSO.   The System Owner must restrict the activities associated with transport of such media to authorized personnel. |
| Part b | All system users must protect, control, and maintain accountability for digital and non-digital media during transport outside of controlled areas using approved resources, techniques, equipment, and procedures for the information system's highest security category defined by Federal Information Security Management Act (FISMA). |
| Part c | All activities associated with the transportation of information system media must be documented. |
| Part d | The System Owner must restrict the activities associated with transport of such media to authorized personnel who have completed at least an SSBI investigation. |

#### MP-5 (4) Control Enhancement (M) (H)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

| MP-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
| The organization must use [FIPS 140-2](https://csrc.nist.gov/publications/detail/fips/140/2/final) compliant cryptographic mechanisms to protect the confidentiality and integrity of the information stored on digital media during transport outside of organizational controlled areas. |

### MP-6 Media Sanitization and Disposal (L) (M)

The organization:

1. Sanitizes [media containing highly restricted data] prior to disposal, release out of organizational control, or release for reuse using [agency approved sanitation techniques] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-6(a)-1: digital and non-digital media containing sensitive information | |
| Parameter MP-6(a)-2: agency approved sanitation techniques | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must sanitize information system media - digital and non-digital, removable or non-removable - prior to: disposal, release out of organizational control, or release for reuse.  Removable digital storage devices must be sanitized prior to connecting such devices to the information system under the following circumstances:   * prior to initial use after purchase * when obtained from unknown sources * when the organization loses a positive chain of custody   The organization will sanitize information system media containing sensitive information using National Security Agency (NSA) guidance ([www.nsa.gov/ia/guidance/media\_destruction\_guidance/index.shtml](http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml)) and [NIST SP 800-88](https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final), Guidelines for Media Sanitization  If media cannot be sanitized after use it must be destroyed.  The organization will track, document, and verify media sanitization and disposal actions. |
| Part b | The organization must employ sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. |

#### MP-6 (2) Control Enhancement (M)

The organization tests sanitization equipment and procedures [annually] to verify that the intended sanitization is being achieved.

MP-6 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Equipment and procedures may be tested or evaluated for effectiveness.

| MP-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-6(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
| The organization must test sanitization equipment and procedures to verify correct performance at least annually. |

### MP-7 Media Use (L) (M) (H)

The organization [prohibits] the use of [portable media] on [all information system components] using [Assignment: organization-defined security safeguards].

| MP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter MP-7-1: prohibits | |
| Parameter MP-7-2: portable media | |
| Parameter MP-7-3: all information system components | |
| Parameter MP-7-4: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-7 What is the solution and how is it implemented? |
| --- |
| The organization prohibits the use of portable media on all information system components. |

#### MP-7 (1) Control Enhancement (M) (H)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

| MP-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-7 (1) What is the solution and how is it implemented? |
| --- |
| The organization prohibits the use of portable storage devices in the information system if such devices have no identifiable owner**.** |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
   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
2. Reviews and updates the current:
   1. Security planning policy [every one (1) year]; and
   2. Security planning procedures [FedRAMP Assignment: at least annually].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter PL-1(a): information system users | |
| Parameter PL-1(b)(1): every one (1) year | |
| Parameter PL-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The SO collaborates with the IAT to develop and document security policies and procedures on behalf of the senior management. The policies are developed based on federal directives, National Institute of Standards and Technology (NIST) guidelines, executive orders, OMB Circulations/Memorandum, and regulations. The SO in coordination with the ISSO must approve the policy and procedure documents before dissemination. After an approval is obtained, the policies and procedure documents must be distributed to information system users. |
| Part b | The organization ensures that the PL policy is reviewed and updated annually. |

### PL-2 System Security Plan (L) (M) (H)

The organization:

1. 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;
   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 decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [appropriate agency personnel];
3. Reviews the security plan for the information system [annually];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter PL-2(b): appropriate agency personnel | |
| Parameter PL-2(c): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Security Plan (SSP) is a means to document security requirements and associated security controls implemented within a given system. SSP also describes, at a high level, how the security controls and control enhancements meet those security requirements. It does not provide a detailed, technical description of the specific design or implementation of the controls/enhancements. A SSP is required for all critical systems and must be consistent with the agency’s enterprise architecture.  The information system’s SSP must meet the following requirements:   1. Explicitly defines the authorization boundary for the system. An authorization boundary identifies all components of an information system authorized for operation by the agency’s Chief Information Officer or delegate, and excludes separately authorized systems to which the information system is connected. 2. Describes the operational context of the information system in terms of mission and business processes 3. Provides the security categorization of the information system including supporting rationale 4. Describes the operational environment for the information system 5. Describes relationships with or connections to other information systems 6. Provides an overview of the security requirements for the system 7. Describes the security controls in place or planned for meeting those requirements, including a rationale for tailoring and supplementing decisions 8. Identifies any relevant overlays, if applicable;   The SSP must contain either explicitly or by reference all information required for the secure operation, maintenance, and upgrade to the information system.  Reviews and approves the plan by the authorized representative prior to implementing the plan   1. Distributes copies of the security plan and communicates the plan’s subsequent changes to the appropriate agency personnel 2. Reviews the security plan for the information system on an annual basis 3. Updates the plan to address changes made to the information system/environment of operation, problems identified during plan implementation, or security control assessments 4. Explicitly defines the information system that receives, processes, stores, or transmits restricted or highly restricted data |
| Part b | The System Security Plan shall be made available to all users of the information system and a communication plan must be developed which includes onboarding of new users and notification to users of changes. |
| Part c | The System Security Plan must be reviewed at least annually by the ISSO and System Owner. The System Owner is responsible for ensuring that all internal users have reviewed and are able to comply with the System Security Plan. |
| Part d | The System Security Plan must be updated to address changes made to the information system/environment of operation, problems identified during plan implementation, or security control assessments. |
| Part e | Although the System Security Plan must be made available to all users, specific information within the plan must be restricted based on least-privilege. It is recommended that system specific sensitive information is maintained in separate documents that are included by reference in the SSP. These documents can then be protected by additional security controls.  Changes to the System Security Plan must be managed through the organizations change management process. |

#### PL-2 (3) Control Enhancement (M) (H)

The organization plans and coordinates security-related activities affecting the information system with [other agency entities (departments, divisions, management, etc.] before conducting such activities in order to reduce the impact on other organizational entities.

| PL-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter PL-2(3): other agency entities (departments, divisions, management, etc.) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-2 (3) What is the solution and how is it implemented? |
| --- |
| The organization must plan and coordinate security-related activities with other organizations that rely on the information system for mission or business objectives. Coordination is required for both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.  Notification to other organizations of recurring maintenance can be an acceptable method of coordination.  Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing.  The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. |

### PL-4 Rules of Behavior (L) (M)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior [annually]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter PL-4(c): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Security Plan must clearly document based on role the responsibilities and expected behavior with regard to information and information system usage assigned to users of the information system. These responsibilities must be readily available to users at any time and presented in a way that is easily understood and consumed by the expected audience. These responsibilities and expectations shall be collectively referred to as the Rules of Behavior (ROB).  The organization must ensure the Rules of Behavior (ROB) address the following topics:   * Purpose and Applicability * User Responsibilities * Prohibited Actions |
| Part b | Users of the information system must be presented with the Rules of Behavior and provide a signed acknowledgment indicating that they have read, understand, and agree to abide by the rules of behavior before being authorized for access to information and the information system. |
| Part c | The Rules of Behavior must be reviewed and updated if needed at least annually. It is also recommended that the ROB be reviewed as part of any after action process that includes an undesirable action by a user. |
| Part d | When the Rules of Behavior are updated, Users of the information system must be presented with the updated Rules of Behavior including a brief explanation of any changes and provide a signed acknowledgment indicating that they have read, understand, and agree to abide by the updated rules of behavior before being authorized for access to information and the information system. |

#### PL-4 (1) Control Enhancement (M) (H)

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.

| PL-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-4 (1) What is the solution and how is it implemented? |
| --- |
| The organizations rules of behavior must explicitly include restrictions on the use of social media/networking sites and posting organizational information on public websites. Users must be provided with guidance on the use of social media to minimize the risk of accidental data exposure as well as social engineering attacks. |

### PL-8 Information Security Architecture (M) (H)

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. Reviews and updates the information security architecture [annually] to reflect updates in the enterprise architecture; and

PL-8 (b) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, on Page F-8.

1. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

| PL-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter PL-8(b): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Organization must develop and document an information security architecture for the information system. The Information System Architecture is part of the SSP and describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information. It should provide context and guidance for users when interpreting the more detailed requirements in the System Security Plan and specific Security Procedures.  The information security architecture should be integrated into and support the organization’s enterprise architecture. The SSP should explicitly document how the Information System Architecture support’s the goals of the organizations enterprise architecture  The SSP must include any information security assumptions about, and dependencies on, external services used by the information system. |
| Part b | The information security architecture must be reviewed at least annually and whenever the System Security Plan is reviewed. The information security architecture must also be reviewed and updated to reflect changes in the organizational enterprise architecture. |
| Part c | Any review or updates to the system security architecture must also include verification that the information security architecture is reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

1. 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
2. Reviews and updates the current:
   1. Risk assessment policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: System owner and information assurance team | |
| Parameter RA-1(a): developers, system administrators, project managers, information assurance team, information security officer, and system owner | |
| Parameter RA-1(b)(1): at least every three years | |
| Parameter RA-1(b)(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| RA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The SO collaborates with the IAT to develop and document security policies and procedures on behalf of senior management. The policies are developed based on NIST guidelines, FedRAMP and the Department of Defense’s regulations and guidance. The policy is then to be disseminated to developers, system administrators, project managers, information assurance team, information security officer and the system owner. |
| Part b | The organization ensures that the RA policy is reviewed and updated at least every three years. The RA procedures are to be reviewed and updated annually. |

### RA-2 Security Categorization (L) (M) (H)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: CIO, ISSO, system owner, business owners and information owners | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization shall categorize information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The organizations needs to consider potential adverse impacts to other organizations and in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. |
| Part b | The security categorization results (including all supporting rationale) must be documented in the security plan for the information system. |
| Part c | The organization must ensure that the Authorizing Official reviews and approves the security categorization decision. The ISSO is responsible for ensuring that the AO understands the rationale and impact of the security categorization decision. |

### RA-3 Risk Assessment (L) (M)

The organization:

1. 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;
2. Documents risk assessment results in [Selection: security plan; risk assessment report; [FedRAMP Assignment: security assessment report]];
3. Reviews risk assessment results [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs];
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
5. Updates the risk assessment [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs] 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.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

RA-3 (d) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter RA-3(b): in a security assessment report | |
| Parameter RA-3(c): in accordance with OMB A-130 requirements or when a significant change occurs | |
| Parameter RA-3(d): ISSO, information assurance team, system owner, and the Authorizing Official | |
| Parameter RA-3(e): in accordance with OMB A-130 requirements or when a significant change occur | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must conduct a risk assessment which includes the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and its components as part of normally scheduled security assessments. |
| Part b | The results of the risk assessment are to be documented in the Security Assessment Report to include risks considered, mitigations identified, and an explanation of any residual risk. |
| Part c | Risk assessment results are to be reviewed in accordance with OMB A-130 requirements or when a significant change occurs. |
| Part d | The results of a risk assessment must be distributed to the ISSO, information assurance team, system owner, and the Authorizing Official. Results may be shared, in whole or in part, with others but should be protected using least privilege principles. Risk assessment results by definition provide an attack plan against the information system. All necessary precautions must be employed to ensure the protection of this information. |
| Part e | Risk assessments are to be updated in accordance with OMB A-130 requirements or when a significant change occurs. |

### RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

RA-5 (a) Additional FedRAMP Requirements and Guidance:

Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote 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 and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery], in accordance with an organizational assessment of risk; and
4. 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).

RA-5 (e) Additional FedRAMP Requirements and Guidance:

Requirement: To include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-5 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Vulnerability Scanning Requirements

<https://www.FedRAMP.gov/documents/>

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSM and information assurance team | |
| Parameter RA-5(a): monthly and when new vulnerabilities are reported which potentially affect the information system | |
| Parameter RA-5(d): informational as applicable, low risk within 30 days, moderate within 30 days, high risk within 15 days and critical risks within 72 hours | |
| Parameter RA-5(e): key personnel which include the ISSO, IAT, SO and AO. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must scan for vulnerabilities in the information system and host applications at least monthly and when new vulnerabilities are reported which potentially affect the information system. |
| Part b | The organization shall avoid the blinky box syndrome. Tools used for vulnerability assessment shall be carefully reviewed and selected to ensure interoperability. Duplicative tools that provide no unique benefit shall not be employed as part of a holistic vulnerability scanning process. |
| Part c | The organization must Analyze vulnerability scan reports and results from security control assessments to identify legitimate vulnerabilities and determine the correct level of residual risk after taking into account all mitigating factors. |
| Part d | The organization will remediate legitimate vulnerabilities in accordance with an internal assessment of risk approved by the ISSO. Once a vulnerability has been categorized, the organization must remediate the vulnerability in the timeframe listed in the table below based on the risk level:   |  |  | | --- | --- | | **Risk Level** | **Time to Remediation** | | Critical | 72 hours | | High | 15 days | | Moderate | 30 days | | Low | 30 days | | Informational | As applicable |   The ISSO may approve an alternative timeframe for a specific vulnerability in response to specific circumstances. The alternative timeframe may be shorter or longer than the standard timeframe. |
| Part e | Vulnerability scan reports must be distributed to the ISSO, information assurance team, system owner, and the Authorizing Official. Results may be shared, in whole or in part, with others but should be protected using least privilege principles. Vulnerability scan reports by definition provide an attack plan against the information system. All necessary precautions must be employed to ensure the protection of this information. |

#### RA-5 (1) Control Enhancement (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

| RA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
| The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. The vulnerability scans are to updated as new vulnerabilities are discovered, announced, and scanning methods developed. |

#### RA-5 (2) Control Enhancement (M) (H)

The organization updates the information system vulnerabilities scanned [Selection (one or more): [FedRAMP Assignment: prior to a new scan]].

| RA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter RA-5(2): when new vulnerabilities are identified. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (2) What is the solution and how is it implemented? |
| --- |
| The organization updates the information system vulnerabilities when new vulnerabilities are identified. Scanning tools must check for new vulnerability definitions prior to a new scan and at least monthly. |

#### RA-5 (3) Control Enhancement (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| RA-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (3) What is the solution and how is it implemented? |
| --- |
| Scanning procedures must include output that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked) as well as the results of the scan. |

#### RA-5 (5) Control Enhancement (M) (H)

The organization includes privileged access authorization to [FedRAMP Assignment: operating systems, databases, web applications] for selected [FedRAMP Assignment: all scans].

| RA-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter RA-5(5)-1: information system and its components | |
| Parameter RA-5(5)-2: scans in certain situations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (5) What is the solution and how is it implemented? |
| --- |
| Scanning for vulnerabilities must be conducted using privileged accounts that have the highest level of access to all operating systems, databases, and web applications*.* This ensures that the broadest range of vulnerabilities can be detected. |

#### RA-5 (6) Control Enhancement (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

| RA-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (6) What is the solution and how is it implemented? |
| --- |
| The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. |

#### RA-5 (8) Control Enhancement (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

RA-5 (8) Additional FedRAMP Requirements and Guidance:

Requirement: This enhancement is required for all high vulnerability scan findings.

Guidance: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

| RA-5 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (8) What is the solution and how is it implemented? |
| --- |
| When a vulnerability is identified the organization takes necessary steps to mitigate any possible impact from an exploitation of this vulnerability before it’s discovery. This can be accomplished in several ways:   1. review historic audit logs from the date the vulnerability was introduced into the system until the date the vulnerability was remediated, 2. search for specific indicators of compromise that conclusively and reliably identify the exploit, and/or 3. redeploy system components or information from known good backups or source code   The ISSO is responsible for determining the required actions. |

## Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [information system users]:
   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
2. Reviews and updates the current:
   1. Security assessment and authorization policy [every calendar year]; and
   2. Security assessment and authorization procedures [every calendar year].

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Assurance Team | |
| Parameter CA-1(a): information system users | |
| Parameter CA-1(b)(1): every calendar year | |
| Parameter CA-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | After an approval is obtained, the policy and procedure document must be disseminated to information system users. |
| Part b | The organization ensures that CA policy is reviewed and updated every calendar year. |

### CA-2 Security Assessments (L) (M) (H)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [Authorizing Official, System Owner, ISSO, FedRAMP PMO and other designated personnel appointed by management].

CA-2 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Annual Assessment Guidance <https://www.fedramp.gov/documents/>

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-2(b): at least annually | |
| Parameter CA-2(d): Authorizing Official, System Owner, ISSO, FedRAMP PMO and other designated personnel appointed by management | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Prior to the authorization of any information system or information system component, the organization shall develop a Security Assessment Plan (SAP). The SAP must be developed by an impartial assessor. If the SAP is for the information system itself it must be developed by a third Party Assessment Organization (3PAO). If the SAP is for a third party component or service being integrated into the information system the SAP may be developed by the IAT.  The SAP must capture the scope of the assessment; list selected security controls and enhancements to be assessed; list devices and procedures to determine effectiveness; list physical and logical environments; and list information about the assessment team and their roles and responsibilities. |
| Part b | Security assessments must be conducted at least annually or whenever a major change is introduced to the information system. Previously developed SAPs may be used if validated and approved by the impartial assessor. |
| Part c | A Security Assessment Report (SAR) must be generated from every assessment. The SAR is developed by the assessment team and may be reviewed and commented on by other parties but MUST reflect in it’s final form the findings and opinions of the assessment team.  The SAR must describe how the system was assessed; list all the weaknesses that were found during assessment; and provide recommended actions to mitigate all weaknesses. The SAR should contain sufficient information to replicate any vulnerability findings. |
| Part d | Copies of the SAR must be provided to the Authorizing Official, System Owner, ISSO, FedRAMP PMO, and other designated personnel defined in the SAP. Since the SAR contains detailed information about the vulnerabilities and weaknesses of the information system it should be controlled and information contained within the SAR should be distributed only as needed. |

#### CA-2 (1) Control Enhancement (L) (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments

CA-2 (1) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

| CA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-2(1): demonstrated independence through such methods as written executive concurrence of the team’s independence or by reporting through an alternative chain of command. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not:   * create a mutual or conflicting interest with the organizations where the assessments are being conducted; * assess their own work; * act as management or employees of the organizations they are serving; or * place themselves in positions of advocacy for the organizations acquiring their services.   Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments.  In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments. |

#### CA-2 (2) Control Enhancement (M) (H)

The organization includes as part of security control assessments, [FedRAMP Assignment: at least annually], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].

CA-2 (2) Additional FedRAMP Requirements and Guidance:

Requirement: To include 'announced', 'vulnerability scanning’ to occur at least annually.

| CA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-2(2)-1: at least annually | |
| Parameter CA-2(2)-2: announced | |
| Parameter CA-2(2)-3: in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment | |
| Parameter CA-2(2)-4: static and dynamic code analysis | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (2) What is the solution and how is it implemented? |
| --- |
| In addition to continuous monitoring requirements which are defined in CA-7, a Security Assessment must be conducted at least annually which includes:   * in-depth monitoring of information system activity for a period of not less than 72 hours to identify any activity that is not in compliance with security policies; * vulnerability scanning of all information system components within the scope of the assessment; * malicious user testing such as phishing exercises or social engineering attempts targeted at information system users identified in the SAP; * insider threat assessment prepared by the independent assessor based on their own observations and information provided by the organization. |

#### CA-2 (3) Control Enhancement (M) (H)

The organization accepts the results of an assessment of [Assignment: organization-defined information system] performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] when the assessment meets [FedRAMP Assignment: the conditions of the JAB/AO in the FedRAMP Repository].

| CA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-2(3)-1: the information system | |
| Parameter CA-2(3)-2: any FedRAMP Accredited 3PAO | |
| Parameter CA-2(3)-3: the conditions of the *JAB/AO* in the FedRAMP Repository | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
| The organization must accept the results of any assessment performed by a FedRAMP Accredited 3PAO when the assessment meets the conditions of the AO as defined in this policy and other related policies. |

### CA-3 System Interconnections (L) (M) (H)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [at least annually].

Table 13‑1. CA-3 Authorized Connections

| **Authorized Connections Information System Name** | **Name of Organization CSP Name System Connects To** | **Role and Name of Person Who Signed Connection Agreement** | **Name and Date of Interconnection Agreement** |
| --- | --- | --- | --- |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-3(c): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | A system interconnection, as defined in this policy, is an approved data flow path between the information system and an external system. The data flow path is permanently available and does not require interaction by a user to transfer data once enabled. For example, an API that is exposed to external users but requires all requests to be processed through the normal system authentication method would not require an interconnection agreement. A persistent VPN connection between the information system and an external system that was used to route multiple kinds of traffic would require an agreement. The organization may allow system interconnections only after a careful consideration of risks introduced by the other system(s).  In the MAX.gov model, the GSS, PaaS, and SaaS layers are all considered part of a single integrated system. An agency specific information system that is deployed on the MAX.gov GSS but which is not open for use by other agencies (and is therefore not included in the MAX.gov Shared Services Boundary) would require an interconnection agreement even if there are no approved data flows between MAX.gov services and the agency specific information system. The two systems are still physically connected even if logically separated so an interconnection agreement is required.  **Authorization of System Interconnections**  The ISSO must review any proposed connections and brief the System Owner and Authorizing Official on any new or modified risks to the information system. The System Owner and ISSO are jointly responsible for ensuring that the Authorizing Official understands any long-term obligations which may result from the agreement including such activities as reporting obligations, responding to data spills or other security events, and additional monitoring which may be required. The Authorizing Official or designated personnel must determine if the risk associated with the information system connection is justified and acceptable.    If interconnecting systems have the same authorizing official, there will be no need to develop Interconnection Security Agreements. Instead, the organization can describe the interface characteristics between those interconnecting systems in their respective system security plans. |
| Part b | Before a system interconnection can be established, the organization must document the characteristics of the connection. These include:   1. The business justification for the connection. 2. The expected source and destination addresses and ports as well as the expected volume and frequency of data transfers. 3. Any security requirements imposed on the external system by the organization, and 4. any security requirements imposed on information system by the external organization. |
| Part c | **Review and Updates of Interconnection Security Agreements**  ISAs must be reviewed and/or updated at least once a year. The System Security Plan (SSP), which must include either explicitly or by reference all Interconnection Security Agreements, should be reviewed monthly to ensure that the ISA information is kept up to date and that the links to the details of each ISA are still accurate. ISAs must be reviewed and updated when there is a change in the system interconnections or when the ISA is close to expiring. |

#### CA-3 (3) Control Enhancement (M) (H)

The organization prohibits the direct connection of an [organization-defined unclassified, non-national security system] to an external network without the use of [boundary protections which meet Trusted Internet Connection (TIC) requirements].

CA-3 (3) Additional FedRAMP Requirements and Guidance:

**Guidance:** Refer to Appendix H – Cloud Considerations of the TIC Reference Architecture document. Link: <https://www.dhs.gov/publication/tic-reference-architecture-22>

| CA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-3(3)-1: unclassified, non-national security system | |
| Parameter CA-3(3)-2: boundary protections which meet Trusted Internet Connection (TIC) requirements | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
| The organization does not allow direct connection of information system components to an external network (such as the Internet) without the use of approved system boundary protection devices. Approved boundary protection devices may be routers or firewalls configured to safeguard information flow between the information system and external networks. This safety mechanism is required for processing, storing, or transmitting any Controlled Unclassified Information (CUI). System architecture component and configurations in place to support boundary protection mechanisms must meet the requirements of Trusted Internet Connections (TIC). |

#### CA-3 (5) Control Enhancement (M)

The organization employs [deny-all, permit by exception] policy for allowing [organization’s information system] to connect to external information systems.

CA-3 (5) Additional FedRAMP Requirements and Guidance:

Guidance: For JAB Authorization, CSPs shall include details of this control in their architecture briefing.

| CA-3 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-3(5)-1: deny-all, permit by exception | |
| Parameter CA-3(5)-2: organization’s information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
| The organization restricts external system connections by employing deny all, permit-by-exception policy to allow connection to external information systems. The purpose is to prevent information system’s connectivity to organizational unapproved external domains or websites. |

### CA-5 Plan of Action and Milestones (L) (M) (H)

The organization:

1. 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
2. Updates existing plan of action and milestones [on a monthly basis] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Plan of Action & Milestones (POA&M) must be provided at least monthly.

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Plan of Action and Milestones (POA&M) Template Completion Guide

[https://www.FedRAMP.gov/documents/](https://www.FedRAMP.gov/resources/documents)

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-5(b): as needed | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must develop and maintain a process for documenting 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. This documentation in summation is the organization’s Plan of Actions and Milestones (POAM). Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.  A POAM entry must be created for any vulnerability or deficiency identified in an accepted Security Assessment Report (SAR) and for any vulnerability identified in the information system which is not corrected in compliance with the timeframes defined in RA-5. |
| Part b | POAMs must be updated as needed whenever new information is available. The ISSO is responsible for ensuring the POAM items are reviewed at least monthly to monitor the organization’s progress in resolving the issue. |

### CA-6 Security Authorization (L) (M) (H)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [on an ongoing basis, providing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation].

CA-6c Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F ([SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-6(c): on an ongoing basis, providing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Organization must select a senior-level executive or manager as the authorizing official for the information system. This individual must be chosen from a group of senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials must provide budgetary oversight for the information system being authorized or assume responsibility for the mission/business operations supported by the system. |
| Part b | The System owner is responsible for ensuring that the system is not processing Government data and information before the system is authorized. The System Owner must receive an official Authorization Letter signed by the AO. |
| Part c | The organization must update the security authorization documentation at least every three years or when a significant change occurs. A significant change is defined as a change that is likely to affect the security state of an information system. Significant changes to an information system may include for example:   * installation of a new or upgraded operating system, middleware component, or application; * modifications to system ports, protocols, or services; * installation of a new or upgraded hardware platform; * modifications to cryptographic modules or services; or * modifications to security controls.   Examples of significant changes to the environment of operation may include for example:   * moving to a new facility; * adding new core missions or business functions; * acquiring specific and credible threat information that the organization is being targeted by a threat source; or * establishing new/modified laws, directives, policies, or regulations.   Keep in mind that these listed examples are only significant when they are likely to affect the security state of the information system. It is ultimately the ISSO who shall determine if a change is significant or not.  When updating security documentation, either due to a scheduled update or in response to a significant change, the organization must review and make necessary updates to all documentation. This includes:   * The System Security plan (SSP) * Any Security Assessment plan (SAP) that is related to a planned or ongoing assessment * Any impacted items in the Plan of Action and Milestones (POAM) * Any Security Assessment Report (SAR) that is still under development   Once all updates have been completed the System Owner and ISSO must provide a summary to the Authorizing Official for approval. |

### CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [Assignment: organization-defined metrics] to be monitored;
2. Establishment of [monthly] for monitoring and [annually] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [designated management personnel] [every 365 days].

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement: Operating System Scans: at least monthly. Database and Web Application Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Guidance: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Continuous Monitoring Strategy Guide

<https://www.fedramp.gov/documents/>

| CA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-7(a): Vulnerabilities, Accounts, privileged account usage, changes, and POAM progress | |
| Parameter CA-7(b)-1: at least monthly | |
| Parameter CA-7(b)-2: annually | |
| Parameter CA-7(g)-1: IAT, ISSO, CIO, System Owner, Authorizing Official | |
| Parameter CA-7(g)-2: IAT on a daily basis, the ISSO on a weekly basis, CIO and System Owner on a monthly basis, and the AO annually. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must develop and implement a Continuous Monitoring (ConMon) program to facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The organization must assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The ConMon program must include:   * Scanning all information system components including operating systems, databases, and web applications for known vulnerabilities * Review of all privileged accounts to verify that the appropriate roles are assigned and no unnecessary privileges are being granted * Review of privileged account usage to identify any improper or suspicious activity * Assessment of changes to determine if any significant changes have been introduced * Review of POAM items to verify the current status and expected remediation date for each outstanding item.   The ConMon plan must also document the organizations plan for engaging an independent third party assessor at least annually to verify and validate the findings of internal monthly assessments.  Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities should be scaled in accordance with the security categories of information systems. |
| Part b | All ConMon tasks must be completed at least once per month. Tasks performed less often than monthly may not provide timely information. Any tasks documented in the ConMon program to be performed less than monthly must be explicitly approved by the ISSO. To the extent possiable ConMon tasks should be incorporated into everyday workflows so that they are performed continuously and relevant information presented to decision makers is always up to date and accurate.  An independent third party assessment must be performed at least annually. The third party assessor should conduct all normally required ConMon activities to validate and verify internal findings. If the Third Party Assessor and the ISSO agree, ConMon artifacts such as scanning results generated by the internal assessment team may be reviewed by the third party assessor in lieu of performing the tasks again. |
| Part c | The ConMon Program must also verify that the organization is meeting the requirements of security controls selected for the information system. The ConMon program should provide an explicit mapping of ConMon tasks to relevant security controls. |
| Part d | Results of ConMon tasks must be themselves monitored though the ConMon Program. For each task in the ConMon Program the organization must record when the task was performed, by whom, and what the result was. To the extent possible this monitoring should be accomplished through integration with normal workflows and the use of automation. ConMon task status and results must be reviewed at least monthly by the ISSO. |
| Part e | The results of ConMon tasks must be integrated so that results from multiple tasks can be correlated to identify inconsistencies and validate results. |
| Part f | ConMon tasks that identify vulnerabilities, misconfigurations, unauthorized changes, or inappropriate user activity must be documented in POAM items and remediated in compliance with the risk timelines identified in RA-5. |
| Part g | The security state of the information system must be reported to IAT on a daily basis, the ISSO on a weekly basis, CIO and System Owner on a monthly basis, and the AO annually. |

#### CA-7 (1) Control Enhancement (M) (H)

The organization employs assessors or assessment teams with [independence and experience to perform impartial assessment] to monitor the security controls in the information system on an ongoing basis.

| CA-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-7(1): independence and experience to perform impartial assessment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
| The organization must employ an Information Assurance Team to operate as independent assessors of the organization’s compliance with approved policies and procedures. The Information Assurance team’s independence must be guaranteed through such methods as written executive concurrence of the team’s independence or by reporting through an alternative chain of command.  The organization must also retain an external independent assessment team to perform assessments and monitoring of the information system on a regular basis. This must include at a minimum an annual assessment and monthly reviews of closed POAMs.  The IAT team and any external assessors must possesses the level of independence and experience to perform impartial assessment that will benefit the organization’s continuous monitoring program. |

### CA-8 Penetration Testing (M) (H)

The organization conducts penetration testing [at least once a year] on [system hardware, software, and firmware components of the information system].

CA-8 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Penetration Test Guidance

<https://www.fedramp.gov/documents/>

| CA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-8-1: at least once a year | |
| Parameter CA-8-2: system hardware, software, and firmware components of the information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-8 What is the solution and how is it implemented? |
| --- |
| Penetration testing must be conducted at least once a year by a qualified penetration tester. The test must be performed on systems that exactly match the deployed production environment. The scope of the penetration testing should include:   * system hardware, software, and firmware components * physical and technical security controls * user activity such as phishing and social engineering attacks * Any other requirements defined in the Penetration Test Guidance provided by the FedRAMP PMO (See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents > Penetration Test Guidance (https://www.fedramp.gov/documents/) |

#### CA-8 (1) Control Enhancement (M) (H)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| CA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-8 (1) What is the solution and how is it implemented? |
| --- |
| The organization must utilize an independent penetration testing agent or team to conduct penetration testing on the information system. The independent penetration tester must be approved by the ISSO after a review of the agent or team’s qualifications. Independent penetration testers must be experts in the field and provide unbiased assessments on the information system. The ISSO must confirm that independent penetration agents or teams do not have any conflict of interest in the development, operation, or management of the information systems that are the targets of the penetration testing. The organization must utilize only FedRAMP accredited Third Party Organizations (3PAO) as independent penetration testing teams or agents. |

### CA-9 Internal System Connections (L) (M) (H)

The organization:

1. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter CA-9(a): printers, copiers and scanners | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization defines specific interface characteristics and security requirements for the connection of internal system components. For example, application to database connections or server to monitoring systems. Requirements should be defined for classes of connection types and may also be defined for specific system to system connections that have unique requirements. |
| Part b | For each system component of the information system, the organization must document ALL internal connections including the approved connection profile in use, the business justification for the connection, and the nature of the information communicated. |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

1. 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
2. Reviews and updates the current:
   1. System and communications protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and communications protection procedures [FedRAMP Assignment: at least annually].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-1(a): ISSO, project managers, system owners, developers, system administrators, security team and database administrators | |
| Parameter SC-1(b)(1): annually | |
| Parameter SC-1(b)(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization develops, documents, and disseminates SC policy and procedures to its ISSO, project managers, SO, SAs, developers, security team and database administrators. |
| Part b | The organization shall review and update the SC policy and procedures annually. |

### SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-2 What is the solution and how is it implemented? |
| --- |
| The organization shall separate user functionality from management functionality. The purpose for this separation is:   1. To minimize the risk of privilege escalation, and 2. To minimize the risk of a spear fishing or XSS attack against an administrator resulting in a compromise in security   Separation of functionality may be through either physical controls (such as network routing) or logical controls such as requiring a separate account for administrative actions.  Information system management functionality includes functions necessary to administer databases, network components, workstations or servers and typically requires privileged user access.  The specific implementation of this control should consider the impact on the organizations mission as well as the risk mitigation. Frequently accessed administrative functions that would be of limited value to an attacker should not be made unreasonably cumbersome to access in pursuit of this control.  Requiring a strong multi-factor authentication such as a PIV or CAC may provide just as much protection and be easier to implement. |

### SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-4 What is the solution and how is it implemented? |
| --- |
| The information system shall protect shared system resources from being exploited for unauthorized or unintended information transfer or exposure.  The organization will ensure all pertinent data (including encrypted data) is properly stored and permissioned to allow only the appropriate users of that data to access it. The information system will restrict access to temporary data, ensuring that only the appropriate users have access to the data, and removing the data from temporary spaces (such as memory) when it is no longer needed. |

### SC-5 Denial of Service Protection (L) (M) (H)

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].

| SC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-5-1: memory attacks, flood attacks, usage priorities, exceeding quotas and the use of portioning to assist in harming the information system | |
| Parameter SC-5-2: standard MTIPS specified security safeguards | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-5 What is the solution and how is it implemented? |
| --- |
| The information system will protect against or limit the effects of memory attacks, flood attacks, usage priorities, exceeding quotas and the use of partitioning to assist in harming the information system by employing standard MTIPS specified security safeguards.  The organization must also implement segmentation and limitations such as containers, C Groups, or VMs to prevent a DOS attack on shared resources such as system memory, CPU, or other system resources from impacting multiple systems. The information system shall limit the number of connections and terminate any idle connections.  The information system shall be regularly assessed for potential DOS vulnerabilities and any identified vulnerabilities shall be documented and remediated in the time threshold specified in the RA-5 policy. |

### SC-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

| SC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-6-1: CPU, Memory, and Storage | |
| Parameter SC-6-2: quota | |
| Parameter SC-6-3: using Virtualization and OS standard tools | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-6 What is the solution and how is it implemented? |
| --- |
| The information system protects the availability of resources by limiting the resources a process may consume. Virtualization architecture shall be used to limit the resources available to an application. Application resources should be further restricted using standard industry techniques for the specific OS and/or application type.  Some examples of techniques for limiting resource consumption may include:   * Memory caps on each VM and a CPU cap on the number of cores with the hypervisor * Limits on the number of users in the httpd server for web access * Use IP tables to track simultaneous connections per user IP and drops or rejects SYN packets above a limit * At the network boundary, IP tables may be configured to limit the number of sessions a given user can setup concurrently * Inside the application server a reasonable memory limit should be set for Java applications and C group limitations serve the same purpose for rails applications |

### SC-7 Boundary Protection (L) (M) (H)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-7(b): physically | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All data crossing the information system boundary must traverse a controlled security device (such as a firewall) and be inspected. For inbound traffic this inspection should occur before data is allowed access to information system resources or components.  As data traverses the internal network it should be monitored whenever it passes between information system components which serve different business functions. Internal security devices must be configured to minimize lateral movement within the information system and should enforce the most restrictive set of rules possible which still allow normal operation of the specific components they are protecting. |
| Part b | Internal management tools MUST be hosted on distinct physically separated networks from publicly accessible user facing systems. Subnetworks shall be used to further segment information system components based on business roles. |
| Part c | All outbound traffic must also be routed through controlled security devices. Outbound traffic should be permitted only as needed for normal information system functionality. Outbound traffic shall be inspected for evidence of data exfiltration or other indicators of compromise. |

#### SC-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

| SC-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (3) What is the solution and how is it implemented? |
| --- |
| The information system limits the number of external network connections to the information system at the outer edge of the security boundary and at key points within the information system network. Limitations should be configured based on expected usage of the information system and adjusted regularly in response to changing usage patterns. |

#### SC-7 (4) Control Enhancement (M)

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [FedRAMP Assignment: at least at least annually] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-7(4)(e): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization will implement a managed interface for each external telecommunication service, implement a traffic flow policy for each managed interface, and protect the confidentiality and integrity of the information being transmitted across each interface using at a minimum TLS 1.2. |
| Part b | The organization will implement a traffic flow policy for each managed interface based on the expected volume and type of traffic anticipated or historically observed. |
| Part c | The organization will protect the confidentiality and integrity of the information being transmitted across each interface using TLS 1.2 encryption or equivalent. |
| Part d | Any exception to the traffic flow policy must be documented with supporting mission/business need and duration of that need. Exceptions must be approved by the System owner and the ISSO. |
| Part e | The organization will review exceptions to the traffic flow policy annually (at the minimum) and remove exceptions that are no longer supported by an explicit mission/business need. |

#### SC-7 (5) Control Enhancement (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| SC-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
| The information system, at managed interfaces, shall employ a deny all and permit by exception policy. Specific traffic shall be permitted only as required by the organization’s business/mission needs and risk management framework. |

#### SC-7 (7) Control Enhancement (M) (H)

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.

| SC-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (7) What is the solution and how is it implemented? |
| --- |
| The information system, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resource external networks. This is commonly referred to as “split-tunneling”.  Remote connections to the information system should be proxied through an https connection and are therefore sandboxed by the browser or through a similar sandboxed protocol such as Citrix. Direct connection of a remote resource over a VPN should be restricted to only the most trusted users and only for business needs that cannot be met through other means. |

#### SC-7 (8) Control Enhancement (M) (H)

The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

| SC-7 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-7(8)-1: | |
| Parameter SC-7(8)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (8) What is the solution and how is it implemented? |
| --- |
| The information system routes all outbound traffic through external proxies which restrict traffic to whitelisted domains based on the source IP address. This effectively mitigates any risk of data exfiltration, reverse shells and similar vulnerabilities. Due to the highly restrictive whitelisting additional security achieved through requiring authentication would not provide any significant increase in security while introducing significant complexity and possibility for unintended service disruption. |

#### SC-7 (12) Control Enhancement (M)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [Assignment: organization-defined information system components].

| SC-7 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-7(12)-1: host based firewalls and other host based boundary protection mechanisms | |
| Parameter SC-7(12)-2: organizational defined information system components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
| To the extent possible, information system hosts must be configured to enforce the same least functionality rules enforced within the information system network. Host based firewalls should be configured to deny all outbound and inbound connections that are not strictly required for normal operation. Unused protocols should be rejected/disabled and unnecessary interfaces/ports must be closed. |

#### SC-7 (13) Control Enhancement (M)

The organization isolates [FedRAMP Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7 (13) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

| SC-7 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-7(13): computer network defense, monitoring, assessment and other security system components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (13) What is the solution and how is it implemented? |
| --- |
| The organization isolates computer network defense, monitoring, assessment and other security system components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system. The intention of this control is to prevent an attacker from disabling security components or using security tools to attack other system components. |

#### SC-7 (18) Control Enhancement (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

| SC-7 (18) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
| The information system fails securely in the event of operational failure of a boundary protection device, so when the information system has an operational failure, the information system stops working. Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the information system, nor can failures permit unauthorized information releases. |

### SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

| SC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-8: confidentiality and integrity | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-8 What is the solution and how is it implemented? |
| --- |
| The information system shall protect both the confidentiality and integrity of transmitted information. This control applies to both internal and external networks of all types of information system components from which information can be transmitted such as servers, mobile devices, printers, copiers, and scanners.  Physical and logical means may be used to protect the confidentiality and integrity of organizational information. An example of a physical mean would be hosting the information system within a secure government data center. And an example of a logical mean would be employing encryption techniques.  If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness the organizations must implement appropriate compensating security controls and explicitly accept any residual risk. Residual risk must be determined by the ISSO, documented and specifically approved by the Authorizing Official. |

#### SC-8 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to [FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information] during transmission unless otherwise protected by [FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)].

| SC-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-8 (1)-1: prevent unauthorized disclosure of information and detect changes to information | |
| Parameter SC-8 (1)-2: by approved physical means | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-8 (1) What is the solution and how is it implemented? |
| --- |
| The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. All data transmitted to or from the information system MUST be encrypted. Internal data transfer MUST be encrypted unless otherwise protected by approved physical means. |

### SC-10 Network Disconnect (M)

The information system terminates the network connection associated with a communications session at the end of the session or after [FedRAMP Assignment: no longer than thirty (30) minutes for RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-10: no longer than thirty (30) minutes for interactive user sessions and no longer than sixty (60) minutes for non-interactive user sessions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-10 What is the solution and how is it implemented? |
| --- |
| The information system is to terminate the network connection associated with a communication session at the end of the session. The information system shall terminate a network connection after no longer than thirty (30) minutes for interactive user sessions and no longer than sixty (60) minutes for non-interactive user sessions if no activity is detected. |

### SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

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].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

| SC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-12: industry best practices and Federally approved and validated cryptography | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 What is the solution and how is it implemented? |
| --- |
| The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the organization’s procedures. All keys must use Federally approved and validated cryptography. Organization procedures for managing keys should reflect the best practices currently used in industry and must meet or exceed the recommended practices of software or hardware providers.  If there is a suspected compromise of a cryptographic key, then a new key must generated and re-issued and the old key must be disabled.  Only live keys are to be stored on servers with access available only to SAs. Keys must be deleted after they are no longer live. |

#### SC-12 (2) Control Enhancement (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [FedRAMP Selection: NIST FIPS-compliant] key management technology and processes.

| SC-12 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-12 (2): NIST FIPS compliant and NSA approved | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 (2) What is the solution and how is it implemented? |
| --- |
| The organization produces, controls, and distributes symmetric cryptographic keys using NIST FIPS compliant and NSA approved key management technology and processes.  Symmetric cryptographic keys typically provide much better performance in data transfer. However, due to the complexity of key management, symmetric cryptographic keys should be used only when there is a specific business need for increased performance. |

#### SC-12 (3) Control Enhancement (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].

| SC-12 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-12 (3): NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 (3) What is the solution and how is it implemented? |
| --- |
| The organization produces, controls, and distributes asymmetric cryptographic keys in a way that provides assurance to the receiver of the public key that the true owner of the key is known (i.e., the claimed owner is the actual owner); this requirement may be disregarded if anonymity is acceptable. However, the strength of the overall architecture and trust in the validity of the protected data depends, in large part, on the assurance of the public-key owner’s identity.  In addition, the distribution of the public key shall provide assurance to the receiver that:   * + - 1. The purpose/usage of the key is known (e.g., for RSA digital signatures or elliptic- curve key agreement),       2. Any parameters associated with the public key are known (e.g., domain parameters),       3. The public key is valid (e.g., the public key satisfies the required arithmetical properties), and       4. The owner actually possesses the corresponding private key   Production, control, and distribution of asymmetric cryptographic keys must be performed using one of the following:   * An NSA-approved key management technology and processes; * An approved PKI Class 3 certificate or prepositioned keying material; * An approved PKI Class 3 or Class 4 certificates; or * hardware security tokens that protect the user's private key |

### SC-13 Use of Cryptography (L) (M) (H)

The information system implements [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-13: FIPS-validated or NSA-approved cryptography | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-13 What is the solution and how is it implemented? |
| --- |
| The information system must use cryptographic protections which comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and are either FIPS-validated or NSA-approved cryptography*.*  The organization shall define and document one or more standard solutions for cryptography. These standardized solutions should be used in all cases. If a particular system component requires some other cryptographic solution this shall be documented as an exception to policy and approved by the System Owner and the ISSO. |

### SC-15 Collaborative Computing Devices (M) (H)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[FedRAMP Assignment: no exceptions]; and
2. Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-15(a): no exceptions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system prohibits remote activation of collaborative computing devices such as networked white boards, cameras, and microphones. Activation of such devices must be initiated by a user physically present with the device and with appropriate authorization. |
| Part b | Collaborative computing devices such as networked white boards, cameras, and microphones shall provide a visual indication to users in the physical vicinity when they are active. |

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | If a system component may allow the use of collaborative computing devices in some circumstances then the devices should be disabled in such a way as to be easily re-enabled by a user with appropriate authorizations. For example, disabling the internal microphone on a laptop through software is preferable to physically disconnecting the device from the motherboard if there is a possibility that the microphone may be used at some future date. |

### SC-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

| SC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SC-17: organizational defined certificate policy | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-17 What is the solution and how is it implemented? |
| --- |
| The organization shall issue certificates for access to information system components by privileged users. Certificates expire every ninety (90) days, and are issued through an automated process that requires a PIV login, and certificate management by the organization super user.  For all certificates, the organization shall manage information system trust stores to ensure only approved anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems such as application-specific time services. |

### SC-18 Mobile Code (M) (H)

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The oranization must implement a tamper protection program for the information system, system component, or information system service to protect the Information System from mobile code that performs unauthorized or malicious actions. The following are categories of mobile code/active content:  **Category 1** - high risk mobile code technologies which exhibit a broad functionality, allowing unmediated access to workstation, server and remote system services and resources. These pose a significant risk to information systems because they allow unlimited access to the host computer. There are two subgroups of Category 1 mobile code technologies:  **Category 1A** technologies can differentiate between signed and unsigned mobile code. The technologies can also be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code.  **Category 1B** technologies cannot differentiate between signed and unsigned mobile code or cannot be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code.  Category 1 mobile code must be obtained from a trusted source and must be signed with an approved PKI code-signing certificate.  To the extent possible, all information system components capable of executing mobile code must be configured to disable the execution of unsigned Category 1 mobile code.  **Category 2** - medium risk mobile code technologies have full functionality, allowing mediated or controlled access to workstations, servers, and remote system services and resources. Category 2 technologies can pose a moderate security threat to information systems because they offer limited control by the user on what the code is allowed to do.  Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel (i.e., TLS VPN, IPsec, or other approved by the ESRMO).  Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, or network connections other than to its originating host).  Where possible, web browsers and other mobile code-enabled products must be configured to prompt the user prior to the execution of Category 2 code.  Where possible, protections against malicious Category 2 technologies must be employed at end user systems and at system boundaries.  **Category 3** - low risk mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 technologies pose limited risk to information systems because they are very restricted in the actions they can perform.  **Emerging mobile code** - all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and therefore have not been assigned to one of the three risk categories described above. |
| Part b | **Category 1A** mobile code technologies may be used when additional restrictions are implemented. The following are assigned to Category 1A:   * ActiveX controls * Shockwave movies (e.g., dcr, .dxr, .dir files), including Xtras, that execute in the Shockwave for Director plug-in.   **Category 1B** mobile code technologies are prohibited from use on the information systems. The following are assigned to Category 1B:   * + - Mobile code scripts that execute in Windows Scripting Host (WSH) (e.g., JavaScript or VBScript downloaded via URL file reference or email attachments)     - Hypertext Mark-up Language (HTML) applications (e.g., .hta files) that download as mobile code, except as part of an approved [MAX.gov](http://max.gov/) application     - Scrap objects (e.g., .shs and .shb files)     - Microsoft Disk Operating System (MS-DOS) batch scripts     - UNIX shell scripts     - Binary executables (e.g., .exe files) that download as mobile code   **Category 2** mobile code may be used when additional restrictions described in <procedure reference> are implemented. Category 2 mobile code should be obtained from a trusted source over an assured channel (i.e., TLS VPN, IPsec, or other approved by the ESRMO).  Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network resources (e.g., file system, Windows registry, or network connections other than to its originating host).  The following are assigned to Category 2:   * + - Java applets and other Java mobile code, except as part of an approved MAX.gov application     - Visual Basic for Applications (VBA) (e.g., Microsoft Office macros)     - LotusScript (e.g., Lotus Notes scripts)     - PerfectScript (e.g., Corel Office macros)     - Postscript     - Mobile code executing in .NET Common Language Runtime   **Category 3** mobile code may be freely used without restrictions in information systems. The following are assigned to Category 3:   * + - JavaScript, including Jscript and European Computer Manufacturers Association (ECMA) Script variants, when executing in the browser     - VBScript, when executing in the browser     - Portable Document Format (PDF)     - Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash plug-in   Emerging mobile code technologies must not be used unless approved by the ISSO. The download and execution of mobile code using emerging technologies must be blocked by all means available at the network boundary, workstation, host, and within applications. |
| Part c | When mobile code is used within the information system it must be explicitly authorized through the configuration management process, monitored for unapproved changes once deployed, and controlled to prevent the execution of mobile code using the same technology which has not been approved. |

### SC-19 Voice Over Internet Protocol (M) (H)

The organization:

1. 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
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization does not support or allow the use of Voice over Internet Protocol (VoIP) technologies. |
| Part b | The organization does not support or allow the use of Voice over Internet Protocol (VoIP) technologies. |

### SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. 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.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system uses DNSSEC. The organization will provide additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries with DNSSEC. |
| Part b | The organization will also provide DNS support with DNSSEC, which includes 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. |

### SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

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.

| SC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-21 What is the solution and how is it implemented? |
| --- |
| The information system will use DNSSEC to request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. Each user of name resolution services either performs this validation on his/her own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local users include recursive resolving or caching domain name system (DNS) servers. DNS user resolvers either perform validation of DNNSEC signatures, or users use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. |

### SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-22 What is the solution and how is it implemented? |
| --- |
| The information system must utilize name and address resolution services that are fault tolerant, and also implement internal and external role separation.  To eliminate single points of failure and to enhance redundancy, organizations shall employ at last two authoritative domain name system servers, one figured as the primary server and the other configured as the secondary server. If these servers are hosted by the organization they must be deployed in two geographically separated subnetworks, not located in the same physical facility.  DNS servers with internal roles only process name and address resolution information requests from clients internal to organization. The organization will specify which users can access authoritative DNS servers in a particular role by address ranges and explicit lists. |

### SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-23 What is the solution and how is it implemented? |
| --- |
| This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. The use of encryption during transit along with implementation of industry best practices to prevent session hijacking (such as http-only cookies with same-origin policy) shall be used to protect the integrity of the session. |

### SC-28 Protection of Information at Rest (M) (H)

The information system protects the [FedRAMP Selection: confidentiality AND integrity]] of [Assignment: organization-defined information at rest].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

| SC-28 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-28-1: confidentiality and integrity | |
| Parameter SC-28-2: data at rest | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-28 What is the solution and how is it implemented? |
| --- |
| The information system must employ encryption to prevent modification or exposure of data when it is at rest. At a minimum, the information system shall employ OS or hardware level disk encryption which prevents a user from modifying or reading data without proper authorization. Additional layers of encryption may be used to protect specific data in accordance with the impact of unauthorized modification or exposure. The ISSO shall determine when additional layers of encryption are required. |

#### SC-28 (1) Control Enhancement (M)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [*Assignment: organization-defined information system components*]

| SC-28 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SC-28(1)-1: all information | |
| Parameter SC-28(1)-2: information system components in operational environment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-28 (1) What is the solution and how is it implemented? |
| --- |
| The information system must employ encryption to prevent modification or exposure of data when it is at rest. At a minimum, the information system shall employ OS or hardware level disk encryption which prevents a user from modifying or reading data without proper authorization. Additional layers of encryption may be used to protect specific data in accordance with the impact of unauthorized modification or exposure. The ISSO shall determine when additional layers of encryption are required. |

### SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-39 What is the solution and how is it implemented? |
| --- |
| Information systems must maintain separate execution domains for each executing process by assigning each process a separate address space.  Each information system process must utilize a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.  This capability is available in most commercial operating systems that employ multi-state processor technologies. The organization shall confirm that these protections are enabled in all baseline configurations. |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

1. 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
2. Reviews and updates the current:
   1. System and information integrity policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and information integrity procedures [FedRAMP Assignment: at least at least annually].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SI-1(a): the systems administrator, project managers, project leads, information assurance team, developers, information systems security officer and quality assurance members | |
| Parameter SI-1(b)(1): every three (3) years | |
| Parameter SI-1(b)(2): annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization develops, documents and disseminates the SI policy and procedures to the systems administrator, project managers, project leads, information assurance team, developers, information systems security officer and quality assurance members. The policy addresses purpose, scope, role, responsibilities, management commitment, coordination among organizational entities and compliance. |
| Part b | The organization will ensure the SI policy is reviewed at least every three (3) years and the procedures are reviewed annually.  For AIX patching, IBM’s periodic patches will be applied within two (2) weeks of their release. Critical security patches are to be applied within seventy-two (72) hours of their release. |

### SI-2 Flaw Remediation (L) (M) (H)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [FedRAMP Assignment: thirty 30 days of release of updates] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Technology Services, IA | |
| Parameter SI-2(c): thirty 30 days of release of updates | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization maintains baseline configuration specifications for all information system components that have been assessed and verified to provide an adequate level of protection. The information System and all of it’s components must be inspected at least weekly to confirm that the deployed configuration in the production environment matches the defined baseline configuration.  The organization must also assess all system components at least weekly to identify any components that are affected by new security vulnerabilities that have been identified. An active subscription to a reliable vulnerability database must be maintained and updated at least daily.  Any deviations from the baseline configuration or identifications of new vulnerabilities must be documented within 24 hours of detection and remediated within the time thresholds specified in the organizations Risk Assessment Policy (RA-5). The remediation process must be centrally managed by the organization such that all flaws are documented in a consistent fashion and made available to relevant stakeholders.  The status of all flaws should be reviewed daily by the information assurance team and any major changes in risk should be communicated to the System Owner. Corrections to flaws may include installing software patches, service packs, and hot fixes; disabling functions, ports, protocols, and services; removing software; and changes to configuration settings. |
| Part b | The organization must evaluate and when possible test updates to the software and firmware related to flaw remediation for effectiveness and potential side effects before installation. |
| Part c | Security-relevant software and firmware updates are to be remediated within the time thresholds specified in the organizations Risk Assessment Policy (RA-5). |
| Part d | Flaw remediation must be incorporated into the organization’s configuration management process.   * All changes made to remediate flaws must follow the organizations configuration management process. * Changes must be reviewed as part of the configuration management process to ensure they do not introduce any new flaws into the information system * Change requests should be rejected if they make changes to an information system component that has known flaws unless the change addresses the flaw. * Once updates are made to remedy a flaw, older versions of software or firmware which contain the flaw should be deleted from the system. |

#### SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [FedRAMP Assignment: at least monthly] to determine the state of information system components with regard to flaw remediation.

| SI-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: IA | |
| Parameter SI-2 (2): at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 (2) What is the solution and how is it implemented? |
| --- |
| The organization must maintain an automated capability which inspects the information system and determines the state of information system components with regard to flaw remediation. An automated process must run at least monthly. The output of this process must include:   * Date and time the report was run * Date and time of last run * Inventory of all system components inspected * Current number of flaws including severity * Number of flaws identified since last run * Number of flaws remediated since last run * A complete listing of all un-remediated flaws including the date the flaw was first identified and the planned date for remediation |

#### SI-2 (3) Control Enhancement (M) (H)

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

| SI-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, ISSO | |
| Parameter SI-2(3)(b): see below | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must monitor the time it takes from identifying a flaw until remediation action is completed. If remediation is not completed within the timeframes specified in this control, the System owner must create a POAM to track remediation efforts until completed. POAMs should be reviewed at least quarterly to identify ways to improve response time. |
| Part b | The organization shall remediate vulnerabilities within the time thresholds specified in RA-5:   1. Seventy-two (72) hours of the update’s release, if vulnerabilities are critical 2. Thirty (30) business days, if vulnerabilities are high 3. Thirty (30) business days of update’s release, if vulnerabilities are moderate/medium 4. Thirty (30) business days of the update’s release, if vulnerabilities are low 5. As applicable, if informational |

### SI-3 Malicious Code Protection (L) (M)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [FedRAMP Assignment: to include alerting administrator or defined security personnel] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SI-3(c)(1)-1: daily | |
| Parameter SI-3(c)(1)-2: intermittent points within the network as well as at endpoints | |
| Parameter SI-3(c)(2): alert the organization’s system administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization shall employ malicious code protection mechanisms such as anti-virus and intrusion detection platforms at the information system’s entry and exit points to detect and eradicate malicious code. |
| Part b | Malicious code protection mechanisms including definitions are to be updated whenever new releases are available in accordance with the organization’s configuration management policy and procedures. |
| Part c | Malicious code protection mechanism should be configured to:   1. Perform daily periodic scans of the information system, and real time scans of files from external sources as the files are downloaded, opened, or executed in accordance with the organization’s security policy. 2. Quarantine malicious code and send alert notifications to the organization’s SAs |
| Part d | The organization should also address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of the information system. |

#### SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 (1) What is the solution and how is it implemented? |
| --- |
| The organization centrally manages malicious code protection mechanisms to ensure consistency and reduce the risk of tampering. Central management includes planning, implementing, assessing, authorizing, and monitoring the malicious code protection security controls.  Malicious code protection solutions should be deployed using a defense in depth model so that data originating from outside the organization’s security boundary is scanned multiple times. Configurations for anti-virus and intrusion detection platforms should be pushed from central servers and centrally monitored. |

#### SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 (2) What is the solution and how is it implemented? |
| --- |
| The organization automatically updates malicious code protection mechanisms including definitions. The automated process must be configured to create mammal delay between the publication of new definitions and the deployment of the definitions within the information system’s malicious code protection mechanisms. |

#### SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 (7) What is the solution and how is it implemented? |
| --- |
| The information system implements non-signature-based malicious code detection mechanisms. Non-signature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms. |

### SI-4 Information System Monitoring (L) (M) (H)

The organization:

1. 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;
2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
3. 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;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. 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;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. 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]].

SI-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

| SI-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Assurance Team | |
| Parameter SI-4(a)(1): security policy and mission/business needs | |
| Parameter SI-4(b): regular audit reviews and account monitoring | |
| Parameter SI-4(g)-1: results of regular audit reviews and account monitoring | |
| Parameter SI-4(g)-2: System Owner and other teams | |
| Parameter SI-4(g)-3: as needed | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization shall monitor the information system to detect attacks and indicators of potential attacks, in accordance with security policy and mission/business needs. This includes failed attacks beyond a certain threshold as well as any unauthorized local, network and remote connections. |
| Part b | The information Assurance team must conduct regular audit reviews and account monitoring of suspicious traffic to identify any unauthorized use of or access to the information system. |
| Part c | Monitoring devices are to be deployed strategically within the information system to collect essential information. These devices should be in addition to other auditing and logging capabilities and serve as a defense in depth measure to capture suspicious behavior in the event other monitoring solutions are compromised.  The deployment of monitoring devices should be evaluated at least annually to ensure the organizations security needs are being met.  Additional monitoring devices should be deployed at ad hoc locations within the system to track specific types of transactions of interest the organization at specific times. For example, in response to a published vulnerability for which a patch does not currently exist. |
| Part d | Monitoring devices deployed under this policy and the information they collect must be protected from unauthorized access, modification, and deletion. These devices are intended, in part, to protect the information system from an internal threat so access to the devices should be limited and when feasible should be assigned in accordance with separation of duties best practices. |
| Part e | The level of the organization’s monitoring activities are to be heightened when there is an indication of an increased risk to the organization’s operations, assets, or data as determined by the ISSO. Monitoring activities shall also be increased when it is determined that such an increase could impact a threat to individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other sources of information. |
| Part f | The information assurance team shall collaborate regularly with the organization’s legal counsel to understand federal laws, Executive Orders, directives, policies, or regulations with regards to information system monitoring activities.  Legal opinion is to be obtained before any major changes in monitoring are implemented. |
| Part g | The information assurance team is to provide malware alerts, unsuccessful log in information, system resource usage and/or custom events related to unmitigated vulnerabilities to the organization team(s) responsible for remediation as the items are detected. |

#### SI-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| SI-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
| Individual intrusion detection tools should be integrated into an information system-wide intrusion detection system to reduce duplication of alerts and to identify inconsistencies which might indicate a miss-configuration or other flaw. |

#### SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (2) What is the solution and how is it implemented? |
| --- |
| The organization employs automation to support near real-time analysis of events captured information system monitoring. This may include both rules-based analysis and advanced analysis techniques such as data modeling and artificial intelligence. Automated analysis must generate notifications to relevant teams and may also be configured to take automated remediation steps. |

#### SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continuously] for unusual or unauthorized activities or conditions.

| SI-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-4(4): continuously | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
| The organization monitors inbound and outbound communication traffic continuously for any unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions include internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. |

#### SI-4 (5) Control Enhancement (M) (H)

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].

SI-4(5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with the incident response plan.

| SI-4 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-4(5)-1: system administrators and the information assurance team | |
| Parameter SI-4(5)-2: Internal traffic indicates the presence of malicious code within the organization’s information systems or propagating among system components; Malware protection detects a threat; Unauthorized export of information | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (5) What is the solution and how is it implemented? |
| --- |
| The information system shall alert the system administrators and the information assurance team when the following indications of compromise or potential compromise occur:   1. Internal traffic indicates the presence of malicious code within the organization’s information systems or propagating among system components 2. Malware protection detects a threat 3. Unauthorized export of information |

#### SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

| SI-4 (14) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
| **The information system does not permit the use of wireless communication devices within the security boundary. Any wireless access point connected to the information system network would be flagged as a rouge device and denied access.** |

#### SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
| The organization correlates information from monitoring tools employed throughout the information system. Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns or inconsistencies that may also be an indicator of compromise or misconfiguration. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. |

#### SI-4 (23) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].

| SI-4 (23) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SI-4(23)-1: organization defined host based monitoring mechanisms | |
| Parameter SI-4(23)-2: servers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (23) What is the solution and how is it implemented? |
| --- |
| The information system baseline configurations must include host-based monitoring mechanisms which contribute to central monitoring data. The specific mechanisms will vary based on the server but must always be defined and explicitly identified in the baseline configuration. |

### SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

1. Receives information system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SI-5(a): designated external organizations on an ongoing basis, such as US CERT, Security focus and Secunia with Splunk. US CERT notifications should be reviewed by the organization as they come out, as well as several pertinent bugtraq/security lists and regular review of security/vulnerability focused news sites | |
| Parameter SI-5(c): SAs, project managers, developers, IAT, federal clients (as appropriate) with security management responsibilities | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization shall receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis. The organization list must include US CERT, any security notification service provided by a product vendor that is part of the information system, and security notifications from external systems with whom a dependency exists. Other sources may be added such as Security focus and Secunia with Splunk, as well as several pertinent bugtraq/security lists and regular review of security/vulnerability focused new sites.  Notifications should be logged, reviewed by the organization, and addressed as appropriate. To the extent possible, automation should be employed to reduce duplicate notifications for the same issue. |
| Part b | If a notification is determined to require some remediation; internal security alerts, advisories and directives must be created and assigned to/communicated to the relevant teams. |
| Part c | The security alerts, advisories and directives are to be disseminated to SAs, project managers, developers, IAT, federal clients (as appropriate). |
| Part d | The organization must implement remediation actions in accordance with established timeframes based on the assessed severity of the issue. If the issue will not be resolved within established timeframes the ISSO must determine if notification to the issuing organization of the degree of noncompliance is appropriate.  For example, notifying an open source project maintainer that the organization has not deployed a patch is likely not an appropriate response. |

### SI-6 Security Functionality Verification (M) (H)

The information system:

1. Verifies the correct operation of [Assignment: organization-defined security functions];
2. Performs this verification [FedRAMP Assignment: to include upon system startup and/or restart at least monthly];
3. Notifies [FedRAMP Assignment: to include system administrators and security personnel] of failed security verification tests; and
4. [Selection (one or more): shuts the information system down; restarts the information system; [FedRAMP Assignment: to include notification of system administrators and security personnel] when anomalies are discovered.

| SI-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-6(a): logging, audit monitoring, and other security related functions | |
| Parameter SI-6(b): at system startup and at least daily | |
| Parameter SI-6(c): system administrators and the organization’s security personnel | |
| Parameter SI-6(d)-1: notifies system administrators and the organization’s security personnel | |
| Parameter SI-6(d)-2: notifies system administrators and the organization’s security personnel | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All components within the information system must verify operation of required logging, audit monitoring, and other security related functions |
| Part b | This verification must occur at system startup and should be verified periodically thereafter but not less than daily. When possible, these functions must be monitored in real time. |
| Part c | In the event that a monitored function fails or cannot be verified System Administrators and the organization’s security personnel are to be notified via email so appropriate action can be taken in response to the alerts. |
| Part d | The information System must be configured to minimize the risk of security functions failing. If possible, security functions must be automatically restarted if they do fail. In general, systems should NOT be configured to shut down or impact availability in response to a failure to validate a security function. |

### SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

| SI-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SI-7: deployed software, system firmware and critical configuration information | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 What is the solution and how is it implemented? |
| --- |
| The organization employs integrity verification tools to detect unauthorized changes to deployed software, system firmware, and critical configuration information.  Verification tools such as AIDE must be used to check the OS and installed packages for any unauthorized changes to deployed binaries and configuration files. Custom software and configurations should be compared to controlled versions maintained in a secure source code repository.  System components must be configured to prevent any unauthorized change and when possible must be configured to replace any changes with the original file to maintain system integrity. |

#### SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events]; [FedRAMP Assignment: at least monthly]].

| SI-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-7(1)-1: deployed software, system firmware and critical configuration information | |
| Parameter SI-7(1)-2: at startup and when a potential indication of compromise is detected | |
| Parameter SI-7(1)-3: at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
| The information system must perform integrity verification of deployed software, system firmware, and critical configuration information at system startup and at least monthly thereafter. The organization must also perform integrity verification checks any time a potential indication of compromise or other relevant security event is detected. |

#### SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

| SI-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SI-7 (7): Unauthorized shutdowns, installation of software, and elevation of user privileges | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (7) What is the solution and how is it implemented? |
| --- |
| Unauthorized shutdowns, installation of software and elevation of user privileges must be explicitly identified in the organization’s incident response capability. Incident response procedures must include notification of security team personnel as well as reverting the system to a safe state. |

### SI-8 Spam Protection (M) (H)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

| SI-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization shall employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages. Information system entry and exit points may include firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and laptop computers. SPAM protection mechanisms must protect users from incoming SPAM and present an attacker from using the information system to send SPAM to a third party. Spam protection mechanisms include rule and signature based scanning as well as secure configuration practices such as SPF and DMARC. |
| Part b | Spam protection mechanisms must be kept current. Signature and pattern definitions must be updated when new releases are available in accordance with organizational configuration management policy and procedures. |

#### SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-8 (1) What is the solution and how is it implemented? |
| --- |
| The organization centrally manages spam protection mechanism. |

#### SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-8 (2) What is the solution and how is it implemented? |
| --- |
| Spam protection mechanisms must be kept current. Signature and pattern definitions must be updated through an automated process when new releases are available |

### SI-10 Information Input Validation (M) (H)

The information system checks the validity of [Assignment: organization-defined information inputs].

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-10: character set, length, numerical range and acceptable values | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-10 What is the solution and how is it implemented? |
| --- |
| The information system shall check the validity of character set, length, numerical range and acceptable values to ensure inputs match specified definitions for format and content. Software applications are to follow well-defined protocols that use structured messages to communicate between software modules or system components. Structured messages may contain raw and unstructured data interspersed with metadata or control information. The module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs are to be completed prior to passing to interpreters to prevent the content from being unintentionally interpreted as commands. Input validation is to help ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks. |

### SI-11 Error Handling (M) (H)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [Assignment: organization-defined personnel or roles].

| SI-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-11(b): personnel authorized to interact with the information system in a test or troubleshooting environment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The information system shall generate error messages to provide information necessary for corrective actions without revealing information that could be exploited by adversaries. In a production deployment complete error messages should be captured in system logs but should NOT be displayed to end users. Error messages must be reviewed as part of any security assessment to ensure they do not contain data that would be useful to an attacker. |
| Part b | The information system may be configured to display raw error messages in any environment where access is limited to those users or staff required to investigate and resolve an issue. This should most often happen in a separate test environment but in certain cases detailed error messages may be allowed in production environment if proper precautions are taken. The ISSO must approve the display of raw error data in the production environment. |

### SI-12 Information Output Handling and Retention (L) (M) (H)

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.

| SI-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-12 What is the solution and how is it implemented? |
| --- |
| The organization handles and retains information within the information system and information system output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Information handling and retention requirements are to cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. |

### SI-16 Memory Protection (M) (H)

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Information system | |
| Parameter SI-16-1: Address-Space Randomization (ASR) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| The information system shall implement Address-Space Randomization (ASR) to protect its memory from unauthorized code execution and to defend against all other memory corruption attacks. The information system will use NX memory flags in the hypervisors and VMs to help prevent buffer overflows and other memory issues. Security safeguards employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

1. 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
2. Reviews and updates the current:
   1. System and services acquisition policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and services acquisition procedures [FedRAMP Assignment: at least annually].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-1(a): system administrators, project managers, SO, developers, database administrators and the security team | |
| Parameter SA-1(b)(1): at least annually | |
| Parameter SA-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization develops, documents and disseminates the SA policy and procedures to the system administrators, project managers, SO, developers, database administrators and the security team. |
| Part b | The organization will ensure the SA policy and procedures are reviewed at least annually. |

### SA-2 Allocation of Resources (L) (M) (H)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. 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
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization will determine required resources for a successful System Security Program by considering all legal and regulatory requirements for the information system as well as risks to the Confidentiality, Integrity, and Availability of the system. |
| Part b | The organization will determine, document and allocate resources required to meet all legal and regulatory requirements identified. Additional resources should be allocated to mitigate risks as deemed appropriate to support the organizations mission. The ISSO must be included in capital planning and investment control process and is responsible for informing other stakeholders of any residual risks and proposing solutions, including cost, to reduce risk. |
| Part c | Once the appropriate resources for the System Security Program have been determined, this funding must be included as a discrete line item for information security in the organizational programming and budgeting documentation. |

### SA-3 System Development Life Cycle (L) (M) (H)

The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO, CIO, security engineers, and security architects | |
| Parameter SA-3(a): system development life cycle | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | A well-defined system development life cycle (SDLC) provides the foundation for the successful development, implementation, and operation of organizational information systems. Individual teams within the organization may develop their own SDLC process to reflect the specific needs and preferences of the team. All SDLC procedures must, at a minimum, meet all of the following requirements:   * The SDLC must be documented in writing and distributed to all members of the team as well as the responsible roles in this policy. * The SDLC must define requirements for deployment of changes to testing **and** production environments that include an assessment of the change for compliance with security policies and procedures * Development of a new SDLC or changes to an existing SDLC must include the ISSO to provide guidance on potential security impacts. |
| Part b | SDLC documentation must specifically identify steps and specific procedures or automation which address system security evaluation and compliance. For example, if the organization or team intends to run automated security tests during the build process it would NOT be sufficient for an SDLC to include a step to “run tests”. Rather a specific step to run “security tests” should be documented including a reference to the applicable tests and how those tests were determined to be sufficient. |
| Part c | Unless otherwise documented in the SDLC, System Security is the responsibility of all team members. If the team wishes to identify only certain team members who have the training and authority to conduct required security assessments this must be clearly documented in the SDLC. All team members must receive appropriate training to implement security roles within the SDLC as determined by the ISSO. |
| Part d | Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.  The ISSO is responsible for ensuring that SDLC procedures address all required organizational information security risk management processes and policies. Any proposed SDLC process which does not meet this requirement must be detailed to the System Owner who is responsible for ensuring necessary changes are made. |

### SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.   
See <http://www.niap-ccevs.org/vpl> or <http://www.commoncriteriaportal.org/products.html>.

| SA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All acquisition contracts must include explicitly or by reference all security functional requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs |
| Part b | All acquisition contracts must include explicitly or by reference all security strength requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs |
| Part c | All acquisition contracts must include explicitly or by reference all security assurance requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs |
| Part d | All acquisition contracts must include explicitly or by reference all security-related documentation requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs |
| Part e | All acquisition contracts must include explicitly or by reference all requirements for protecting security-related documentation in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs |
| Part f | Acquisition contracts must also include a description of the information system environment in which the acquired tool or component is intended to operate. This criteria must provide sufficient information to the vendor so that the vendor can identify and raise any potential security concerns that may be caused by the planned implementation. |
| Part g | Specific acceptance criteria for all acquired tools or components must include compliance with the specified security requirements. |

#### SA-4 (1) Control Enhancement (M) (H)

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.

| SA-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
| During the acquisition process, the vendor must explicitly enumerate how the system, system component, or information system service complies with applicable organizational security policies and procedures. The organization must employ or engage appropriate Subject Matter Experts (SMEs) independent of the proposed vendor who are qualified to evaluate and identify security functions in acquired products. This evaluation must be based on product documentation of functions and features provided by the vendor. The ISSO must also advise the System Owner if additional training or information will be needed by organization users to ensure all security functions are understood and leveraged to the greatest extent feasible. |

#### SA-4 (2) Control Enhancement (L) (M)

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: [FedRAMP Selection (one or more): to include security-relevant external system interfaces, and high-level design]; [Assignment: organization-defined design/implementation information] at [Assignment: organization-defined level of detail].

| SA-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-4-1: security-relevant external system interfaces including interfaces for monitoring, logging and alerting. | |
| Parameter SA-4-2: including at a minimum detailed instructions of how to integrate with existing organizational tools | |
| Parameter SA-4-3: sufficient level of detail to allow the Information Assurance team to accurately assess the impact of the tool or component on the overall information system risk posture and to allow organization staff to successfully integrate with existing tools without additional vendor support | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (2) What is the solution and how is it implemented? |
| --- |
| The organization requires the vendor of any information system, system component, or information system service to provide design and implementation guidance for the security controls to be employed. This guidance must include the purpose and recommended configuration for security-relevant external system interfaces as well as detailed instructions of how to integrate with **existing** organizational tools. Vendors should also provide a high-level design expressed in terms of the interfaces between subsystems providing security-relevant functionality and source code or hardware schematics unless restricted by vendor policy.  The vendor must be able to provide the required guidance at a sufficient level of detail to allow the Information Assurance team to accurately assess the impact of the tool or component on the overall information system risk posture and to allow organization staff to successfully integrate with existing tools without additional vendor support |

#### SA-4 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [FedRAMP Assignment: at least the minimum requirement as defined in control CA-7].

SA-4 (8) Additional FedRAMP Requirements and Guidance:

Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

| SA-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-4(8): sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (8) What is the solution and how is it implemented? |
| --- |
| Vendors must provide a plan for continuous monitoring that includes:   * Notification to the organization of newly discovered vulnerabilities, patches, and updated recommendations for secure configuration and operation * Evaluation of the information system, system component, or information system service by a qualified independent assessor on at least an annual basis * A description of internal processes and policies the vendor has implemented to ensure the security of the information system, system component, or information system service   The organization must include the vendors plan in the organizations continuous monitoring plan. |

#### SA-4 (9) Control Enhancement (M) (H)

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-4 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (9) What is the solution and how is it implemented? |
| --- |
| The organization requires the vendor to identify the functions, ports, protocols and services intended for organizational use early in the system development life cycle or acquisition process. The list of functions, ports, protocols and services must be exhaustive and also represent the minimal requirements for desired functionality. The organization must review and approve the proposed functions, ports, protocols and services before new development or acquisition can be completed. |

#### SA-4 (10) Control Enhancement (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| SA-4 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
| The organization shall implement only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability within the information system. The System Owner or ISSO may approve exceptions to this policy. |

### SA-5 Information System Documentation (L) (M)

The organization:

1. 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;
2. 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;
3. 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;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [Assignment: organization-defined personnel or roles)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-5(c): documents the written acceptance of the Authorizing Official of risks created by any deficiencies in documentation | |
| Parameter SA-5(e): all potential users of the information system as appropriate | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part 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;  Secure configuration parameters must be documented in a machine readable format that can be used by organizational monitoring tools to evaluate current configuration and identify any changes.  Signatures for any known vulnerabilities must be provided in a format that can be used by organization IDS and/or IPS systems. |
| Part 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; |
| Part c | If any of the above information is unavailable or is determined to be insufficient by the ISSO the deficiency must be documented including any attempts taken by the organization to gain or produce the information, projected costs to gain or produce the documentation, and an evaluation of risks created by the documentation deficiency. The Authorizing Official must explicitly accept any risks created by documentation deficiency. |
| Part d | Documentation shall be assessed by the ISSO to determine the FIPS categorization appropriate and must be protected in compliance with the determined FIPS Categorization. The FIPS categorization of documentation may be different (higher or lower) then that of the security category or classification of the information system. |
| Part e | Documentation must be incorporated or included with other information system documentation and distributed to relevant stakeholders. |

### SA-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| SA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Vendor | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-8 What is the solution and how is it implemented? |
| --- |
| The vendor must demonstrate that they apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. The vendor documents web application requirements, which will provide detailed information regarding appropriate documentation of technical development to ensure that they meet the organization’s security requirements and are employing security best practices and using security engineering principles.  Security engineering principles include developing layered protections; establishing a sound security policy, architecture and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that system developers are trained on how to build secure software; tailoring security controls to meet organizational and operational needs; performing threat modeling to identify use cases, threat agents, attack factors, attack patterns, compensating controls and design patters needed to mitigate risk; and reducing risk to acceptable levels. |

### SA-9 External Information System Services (L) (M) (H)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide  
<https://www.FedRAMP.gov/documents>

Guidance: Independent Assessors should assess the risk associated with the use of external services. See the FedRAMP page under Key Cloud Service Provider (CSP) Documents>FedRAMP Authorization Boundary Guidance

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-9(a): security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance | |
| Parameter SA-9(c): an approved vendor continuous monitoring plan | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Providers of external information system services must be provided with documentation of organization information system security requirements and the vendor must comply with the organization’s security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. |
| Part b | The organization must define and document government oversight and user roles and responsibilities with regard to external information system services. |
| Part c | SEE: SA-4(8)  Vendors must provide a plan for continuous monitoring that includes:   * Notification to the organization of newly discovered vulnerabilities, patches, and updated recommendations for secure configuration and operation * Evaluation of the information system, system component, or information system service by a qualified independent assessor on at least an annual basis * A description of internal processes and policies the vendor has implemented to ensure the security of the information system, system component, or information system service   The organization must include the vendors plan in the organizations continuous monitoring plan. |

#### SA-9 (1) Control Enhancement (M) (H)

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

| SA-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-9(1)(b): ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The organization must conducts an assessment of risks which may be introduced by any acquisition or outsourcing of information security services prior to completing any such activity. |
| Part b | Acquisition or outsourcing of information security services must be approved by the ISSO |

#### SA-9 (2) Control Enhancement (M) (H)

The organization requires providers of [FedRAMP Assignment: All external systems where Federal information is processed or stored] to identify the functions, ports, protocols, and other services required for the use of such services.

| SA-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: organization | |
| Parameter SA-9(2): All external systems where Federal information is processed or stored | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (2) What is the solution and how is it implemented? |
| --- |
| The organization requires the vendor to identify the functions, ports, protocols and services intended for organizational use early in the system development life cycle or acquisition process. The list of functions, ports, protocols and services must be exhaustive and also represent the minimal requirements for desired functionality. The organization must review and approve the proposed functions, ports, protocols and services before new development or acquisition can be completed. |

#### SA-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [FedRAMP Assignment: All external systems where Federal information is processed or stored] are consistent with and reflect organizational interests.

| SA-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-9(4)-1: internal security assessments approved by the ISSO | |
| Parameter SA-9(4)-2: All external systems where Federal information is processed or stored | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (4) What is the solution and how is it implemented? |
| --- |
| Prior to the acquisition or incorporation of any external system where federal information will be processed the ISSO or designated official must conduct an evaluation to ensure that the interests of the vendor or provider of the service are consistent with and reflect the interests of the organization. The ISSO must provide this analysis to the System Owner and Authorizing Official prior to acquisition or incorporation. |

#### SA-9 (5) Control Enhancement (M) (H)

The organization restricts the location of [FedRAMP Selection: information processing, information data, AND information services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

Additional FedRAMP Requirements and Guidance

Guidance: System services refer to FTP, Telnet, and TFTP, etc.

| SA-9 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-9(5)-1: : information processing, information data, AND information services | |
| Parameter SA-9(5)-2: secure locations within the United States or it’s territories | |
| Parameter SA-9(5)-3: current government regulations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (5) What is the solution and how is it implemented? |
| --- |
| All information processing, information data storage, and any other information services used by the information systems must be located within secure locations in the United States or it’s territories in compliance with current government regulations. |

### SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [FedRAMP Selection: development, implementation, AND operation];
2. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

SA-10 (e) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: System owners, project managers, developers, system administrators and database administrators | |
| Parameter SA-10(a): development, implementation and operation | |
| Parameter SA-10(b): deployed production instance(s) | |
| Parameter SA-10(e): All organization stakeholder and the security team | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The vendor must demonstrate implementation of effective configuration management of any system, component or service during development, implementation and operation. |
| Part b | Any vendor supplied system, component or service implemented in the information system’s production environment may only be altered in compliance with the organizations configuration management policy. |
| Part c | The vendor may only implement organizational approved changes to the system, component or service. |
| Part d | The vendor is responsible for documenting changes to the system, component, or service and the potential security impacts of such changes. If the change is approved the vendor must document the approval and implementation of the change. |
| Part e | Vendors must track security flaws and flaw resolution and report findings to the organization’s stakeholders and the security team. |

#### SA-10 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

| SA-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-10 (1) What is the solution and how is it implemented? |
| --- |
| Vendors must provide a solution for verifying the integrity of software and firmware received by the organization. For example, checksums or digital signatures may be used to ensure the authenticity and integrity of provided software or firmware. |

### SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Parameter SA-11(b)-1: unit, integration, system, and regression | |
| Parameter SA-11(b)-2: 80% | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Vendors must create and implement a security assessment plan which meets the requirements of the organization |
| Part b | Vendors must perform unit, integration, system, and regression testing of the supplied system, component or service. In aggregate, testing should cover a minimum of 80% of the required system functionality |
| Part c | The vendor must produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation prior to completion of any acquisition or award. |
| Part d | The vendor must implement a verifiable flaw remediation process |
| Part e | The vendor must correct flaws identified during security testing/evaluation as well as flaws reported through the flaw remediation process |

#### SA-11 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 (1) What is the solution and how is it implemented? |
| --- |
| The organization requires the vendor of the information system, system component, or information system service to employ a Static Code Analyzer equivalent to HP Web Inspect in the security analysis of the product. The use of Static Code Analysis for newly developed code must be documented in the vendor’s Continuous Monitoring Plan. |

#### SA-11 (2) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

| SA-11 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 (2) What is the solution and how is it implemented? |
| --- |
| The organization requires the vendor of the information system, system component, or information system service to employ a Threat And Vulnerability Analyses tool equivalent to Tenable Nessus in the security analysis of the product. |

#### SA-11 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

| SA-11 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Organization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 (8) What is the solution and how is it implemented? |
| --- |
| The organization requires the vendor of the information system, system component, or information system service to employ a Dynamic Code Analyzer equivalent to HP Web Inspect in the security analysis of the product. |