FedRAMP™

FedRAMP® System Security Plan (SSP) Appendix A: Low FedRAMP Security Controls

for <Insert CSP Name>

<Insert CSO Name>

<Insert Version X.X>

<Insert MM/DD/YYYY>

TEMPLATE REVISION HISTORY

Date	Version	Pages	Description	Author
06/30/2023	1.0	All	Initial publication. SSP security control sections are now provided as separate templates.	FedRAMP PMO
08/30/2023	1.1	All	Separate parameter fields were added for control sub-parts with multiple parameters. Minor editorial and formatting changes.	FedRAMP PMO

How to contact us

For questions about FedRAMP, or for questions about this document including how to use it, contact info@FedRAMP.gov.

For more information about FedRAMP, see www.FedRAMP.gov.

Delete this Template Revision History page and all other instructional text from your final version of this document.

Appendix A Low: <CSO> FedRAMP Security Controls

Below is the baseline template for the Low impact security controls.

Instructions:

A cloud service provider (CSP) is encouraged to maintain the controls as a separate document from the System Security Plan (SSP) as the size will impact the level of effort needed to review/edit the SSP.

- *The controls tables describe the security controls as they are implemented for the system. For each control, it is important to describe **how** the control is implemented and **from where the control originates** so that it is clear whose responsibility it is to implement, manage, and monitor the control.*
- *Controls inheritance needs to be considered for each control – both from the perspective of a CSP inheriting controls from another CSP and inheritability of controls from a CSP to its customers (agencies or other CSPs). Please see the use case guidance below:*
    - *For controls that are inherited from another CSP, the inheriting CSP should ensure that the "Inherited" box is selected with the name of the CSP being inherited from and that the control solution description states **what** functionality is being inherited from the other CSP.*
        - *Note that "-1" controls (AC-1, AU-1, SC-1, etc.) are **not** 100% inherited; the inheriting CSP must describe their functions to enable inheritance; in some cases, the role may be minimal.*
        - *Please remember that "inheritance" can be claimed from FedRAMP Authorized services only. If a system or service is not FedRAMP Authorized, a CSP is fully responsible for the control (though another entity may perform its function).*
    - *For controls defined as fully inheritable by the customer:*
        - *A CSP is responsible for ensuring its implementation meets federal/FedRAMP control requirements.*

        - *A third party assessment organization (3PAO) is required to validate that inherited security features can be inherited.*
    - *For a control that can only be inherited under a specific use case:*
        - *The CSP must describe that use case in the SSP.*
        - *The 3PAO is required to validate the control inheritability (as dictated by the use case).*
    - *For controls defined as a customer responsibility, agencies are responsible for implementing, documenting, and testing the control.*
    - *For shared responsibility controls:*
        - *Function(s), provided by a CSP, must be clearly documented in the SSP, specifying a CSP's responsibilities AND the responsibilities provided, or configured by, their agency customer.*
        - *A 3PAO is required to test a CSP's responsibilities.*
    - *For all controls, if a CSP provides options for an agency/customer in implementing a control, the CSP must make clear what options are compliant with federal policy.*
    - *A CSP is NOT responsible for having their agency customer's implementation of inherited controls tested.*
    - *A CSP is NOT responsible for having customer-responsible controls tested.*
- *Throughout the controls, policies and procedures must be explicitly referenced (title and date or version and the applicable section or paragraph numbers) so that it's clear which document is being referred to and where, within the document, applicable details can be found.*

Delete this instructional text from your final version of this document.

Instructions:

In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control. In some cases, the responsibility is shared by a

CSP and by their customer. Use the definitions in the table that follows to indicate where each security control originates from. Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version and the applicable section or paragraph numbers) so that it is clear which document is being referred to. Section numbers, or similar mechanisms, should allow the reviewer to easily find the reference.

For SaaS and PaaS systems that are inheriting controls from an IaaS (or anything lower in the stack), the "Inherited" check box must be checked, and the implementation description must simply say "Inherited." FedRAMP reviewers will determine whether the control-set is appropriate or not.

The NIST term, "Organization Defined," must be interpreted as being a CSP's responsibility unless otherwise indicated. In some cases, the JAB has chosen to define or provide parameters, and in others, they have left the decision up to CSPs.

Please note: CSPs should not modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements. CSP responses must be documented in the "Control Summary Information" and "What is the solution and how is it implemented?" tables.

Delete this instructional text from your final version of this document.

The definitions in Table A-1. Control Origination and Definitions indicate where each security control originates.

Table A-1. Control Origination and Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from a CSP's corporate network.	DNS from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular CSP system and the control is	A unique host-based intrusion detection system (HIDs) is available on the service offering

Control Origination	Definition	Example
	not part of the standard corporate controls.	platform but is not available on the corporate network.
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls specific to a particular system.	There are scans of the corporate network infrastructure; scans of databases and web-based applications are system specific.
Configured by Customer	A control where the customer needs to apply a configuration to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http* or https, etc.), entering an IP range specific to their organization are configurable by the customer.
Provided by Customer	A control where the customer needs to provide additional hardware or software to meet the control requirement.	The customer provides a SAML SSO solution to implement two-factor authentication.
Shared	A control that is managed and implemented partially by a CSP and partially by their customer.	Security awareness training must be conducted by both the CSPN and the customer.
Inherited from pre-existing FedRAMP Authorization	A control that is inherited from another CSP system that has already received a FedRAMP authorization.	A PaaS or SaaS provider inherits PE controls from an IaaS provider.

*Hyper Text Transport Protocol (http)

Responsible role indicates the role of a CSP employee who can best respond to questions about the particular control that is described.

TABLE OF CONTENTS

Access Control

AC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

   1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AC-1 Control Summary Information
Responsible Role:
Parameter AC-1(a):
Parameter AC-1(a)(1):

Parameter AC-1(b):
Parameter AC-1(c)(1)-1:
Parameter AC-1(c)(1)-2:
Parameter AC-1(c)(2)-1:
Parameter AC-1(c)(2)-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)

AC-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;

d. Specify:

    1. Authorized users of the system;

    2. Group and role membership; and

    3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];

g. Monitor the use of accounts;

h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

    1. [FedRAMP Assignment: twenty-four (24) hours] when accounts are no longer required;

    2. [FedRAMP Assignment: eight (8) hours] when users are terminated or transferred; and

    3. [FedRAMP Assignment: eight (8) hours] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

    1. A valid access authorization;

    2. Intended system usage; and

3. [Assignment: organization-defined attributes (as required)];

j. Review accounts for compliance with account management requirements [FedRAMP Assignment: at least annually];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

AC-2 Control Summary Information
Responsible Role:
Parameter AC-2(c):
Parameter AC-2(d)(3):
Parameter AC-2(e):
Parameter AC-2(f):
Parameter AC-2(h):
Parameter AC-2(h)(1):
Parameter AC-2(h)(2):
Parameter AC-2(h)(3):
Parameter AC-2(i)(3):
Parameter AC-2(j):
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:
Part f:

Part g:
Part h:
Part i:
Part j:
Part k:
Part l:

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

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

AC-3 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

AC-3 What is the solution and how is it implemented?

AC-7 Unsuccessful Logon Attempts (L)(M)(H)

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection (one-or-more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

AC-7 Additional FedRAMP Requirements and Guidance:

Requirement: In alignment with NIST SP 800-63B.

AC-7 Control Summary Information
Responsible Role:
Parameter AC-7(a)-1:

Parameter AC-7(a)-2:
Parameter AC-7(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Display [FedRAMP Assignment: see additional Requirements and Guidance] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording.

b. Retain 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 system; and

c. For publicly accessible systems:

1. Display system use information [FedRAMP Assignment: see additional Requirements and Guidance], before granting further access to the publicly accessible system;

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

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

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.

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:
Parameter AC-8(a):
Parameter AC-8(c)(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-8 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system user actions not requiring identification or authentication.

AC-14 Control Summary Information
Responsible Role:
Parameter AC-14(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-14 What is the solution and how is it implemented?
Part a:
Part b:

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

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

AC-17 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

AC-17 What is the solution and how is it implemented?
Part a:
Part b:

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

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

AC-18 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

AC-18 What is the solution and how is it implemented?
Part a:
Part b:

AC-19 Access Control for Mobile Devices (L)(M)(H)

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

AC-19 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

AC-19 What is the solution and how is it implemented?
Part a:
Part b:

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

a. [Selection (one-or-more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and

2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [Assignment: organizationally defined types of external systems].

AC-20 Additional FedRAMP Requirements and Guidance:

Guidance: The interrelated controls of AC-20, CA-3, and SA-9 should be differentiated as follows:

AC-20 describes system access to and from external systems.

CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the CSO and an external system.

SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3.

AC-20 Control Summary Information
Responsible Role:
Parameter AC-20(a):
Parameter AC-20(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [FedRAMP Assignment: at least quarterly] and remove such information, if discovered.

AC-22 Control Summary Information
Responsible Role:
Parameter AC-22(d):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:
Part c:
Part d:

Awareness and Training

AT-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] awareness and training policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AT-1 Control Summary Information
Responsible Role:
Parameter AT-1(a):
Parameter AT-1(a)(1):
Parameter AT-1(b):
Parameter AT-1(c)(1)-1:
Parameter AT-1(c)(1)-2:
Parameter AT-1(c)(2)-1:
Parameter AT-1(c)(2)-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)

AT-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

AT-2 Literacy Training and Awareness (L)(M)(H)

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and [FedRAMP Assignment: at least annually] thereafter; and

2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

c. Update literacy training and awareness content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

AT-2 Control Summary Information
Responsible Role:
Parameter AT-2(a)(1):
Parameter AT-2(a)(2):
Parameter AT-2(b):
Parameter AT-2(c)-1:
Parameter AT-2(c)-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

AT-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

AT-2(2) Insider Threat (L)(M)(H)

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-2(2) 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

AT-2(2) What is the solution and how is it implemented?

AT-3 Role-based Training (L)(M)(H)

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities [Assignment: organization-defined roles and responsibilities]:

1. Before authorizing access to the system, information, or performing assigned duties, and [FedRAMP Assignment: at least annually] thereafter; and

2. When required by system changes;

b. Update role-based training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events]; and

c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

AT-3 Control Summary Information
Responsible Role:
Parameter AT-3(a):
Parameter AT-3(a)(1):
Parameter AT-3(b)-1:
Parameter AT-3(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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

AT-4 Training Records (L)(M)(H)

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [FedRAMP Assignment: at least one (1) year or 1 year after completion of a specific training program].

AT-4 Control Summary Information
Responsible Role:
Parameter AT-4(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation

☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

Audit and Accountability

AU-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] audit and accountability policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

AU-1 Control Summary Information
Responsible Role:
Parameter AU-1(a):
Parameter AU-1(a)(1):
Parameter AU-1(b):
Parameter AU-1(c)(1)-1:
Parameter AU-1(c)(1)-2:
Parameter AU-1(c)(2)-1:
Parameter AU-1(c)(2)-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)

AU-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

AU-2 Event Logging (L)(M)(H)

a. Identify the types of events that the system is capable of logging in support of the audit function: [FedRAMP Assignment: 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];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2a to be audited continually for each identified event.];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [FedRAMP Assignment: annually and whenever there is a change in the threat environment].

AU-2 Additional FedRAMP Requirements and Guidance:

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

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

AU-2 Control Summary Information
Responsible Role:
Parameter AU-2(a):
Parameter AU-2(c):
Parameter AU-2(e):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned

☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:

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

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3 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

AU-3 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:
Part f:

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

Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].

AU-4 Control Summary Information
Responsible Role:
Parameter AU-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

AU-4 What is the solution and how is it implemented?

AU-5 Response to Audit Logging Process Failures (L)(M)(H)

a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and

b. Take the following additional actions: [FedRAMP Assignment: overwrite oldest record].

AU-5 Control Summary Information
Responsible Role:
Parameter AU-5(a)-1:
Parameter AU-5(a)-2:

Parameter AU-5(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Review and analyze system audit records [FedRAMP Assignment: at least weekly] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [Assignment: organization-defined personnel or roles]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. 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:
Parameter AU-6(a)-1:
Parameter AU-6(a)-2:
Parameter AU-6(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable

Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

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

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [FedRAMP Assignment: one second granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-8 Control Summary Information

Responsible Role:
Parameter AU-8(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

AU-9 Control Summary Information
Responsible Role:
Parameter AU-9(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
Part a:
Part b:

AU-11 Audit Record Retention (L)(M)(H)

Retain audit records for [FedRAMP Assignment: a time period in compliance with M-21-31] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Guidance: The service provider is encouraged to align with M-21-31 where possible.

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.

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf).

AU-11 Control Summary Information
Responsible Role:
Parameter AU-11:

Implementation Status (check all that apply):

☐ Implemented

☐ Partially Implemented

☐ Planned

☐ Alternative implementation

☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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?

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

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [FedRAMP Assignment: all information system and network components where audit capability is deployed/available];

b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

AU-12 Control Summary Information
Responsible Role:
Parameter AU-12(a):
Parameter AU-12(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

Assessment, Authorization, and Monitoring

CA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and
2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

CA-1 Control Summary Information
Responsible Role:
Parameter CA-1(a):
Parameter CA-1(a)(1):
Parameter CA-1(b):
Parameter CA-1(c)(1)-1:
Parameter CA-1(c)(1)-2:
Parameter CA-1(c)(2)-1:
Parameter CA-1(c)(2)-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:
Part b:
Part c:

CA-2 Control Assessments (L)(M)(H)

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;

2. Assessment procedures to be used to determine control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation [FedRAMP Assignment: 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 and privacy;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to [FedRAMP Assignment: individuals or roles to include FedRAMP PMO].

CA-2 Additional FedRAMP Requirements and Guidance:

Guidance: Reference FedRAMP Annual Assessment Guidance.

CA-2 Control Summary Information
Responsible Role:
Parameter CA-2(d):
Parameter CA-2(f):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:
Part f:

CA-2(1) Independent Assessors (L)(M)(H)

Employ independent assessors or assessment teams to conduct control assessments.

CA-2(1) 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

CA-2(1) What is the solution and how is it implemented?

CA-3 Information Exchange (L)(M)(H)

a. Approve and manage the exchange of information between the system and other systems using [Selection (one-or-more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements, [Assignment: organization-defined type of agreement]];

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements [FedRAMP Assignment: at least annually and on input from JAB/AO].

CA-3 Control Summary Information
Responsible Role:
Parameter CA-3(a):
Parameter CA-3(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:

Part b:
Part c:

CA-5 Plan of Action and Milestones (L)(M)(H)

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [FedRAMP Assignment: at least monthly] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Requirement: POA&Ms must be provided at least monthly.

Guidance: Reference FedRAMP-POAM-Template.

CA-5 Control Summary Information
Responsible Role:
Parameter CA-5(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:

CA-6 Authorization (L)(M)(H)

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

   1. Accepts the use of common controls inherited by the system; and

   2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs].

CA-6 Additional FedRAMP Requirements and Guidance:

(e) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. 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:
Parameter CA-6(e):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:

CA-7 Continuous Monitoring (L)(M)(H)

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];

b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [FedRAMP Assignment: to include JAB/AO] [Assignment: organization-defined frequency].

CA-7 Additional FedRAMP Requirements and Guidance:

Guidance: FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan.

Requirement: Operating System, Database, Web Application, Container, and Service Configuration Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Requirement: CSOs with more than one agency ATO must implement a collaborative Continuous Monitoring (ConMon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing ConMon oversight. It does not apply to CSOs authorized via the JAB path because the JAB performs ConMon oversight.

CA-7 Control Summary Information
Responsible Role:
Parameter CA-7(a):
Parameter CA-7(b)-1:
Parameter CA-7(b)-2:
Parameter CA-7(g)-1:
Parameter CA-7(g)-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

CA-7 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:
Part f:

Part g:

CA-7(4) Risk Monitoring (L)(M)(H)

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

CA-7(4) 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

CA-7(4) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

CA-8 Penetration Testing (L)(M)(H)

Conduct penetration testing [FedRAMP Assignment: at least annually] on [Assignment: organization-defined systems or system components].

CA-8 Additional FedRAMP Requirements and Guidance:

Guidance: Scope can be limited to public facing applications in alignment with M-22-09. Reference the FedRAMP Penetration Test Guidance.

CA-8 Control Summary Information
Responsible Role:
Parameter CA-8-1:
Parameter CA-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

CA-8 What is the solution and how is it implemented?

CA-9 Internal System Connections (L)(M)(H)

a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after [Assignment: organization-defined conditions]; and

d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

CA-9 Control Summary Information
Responsible Role:
Parameter CA-9(a):
Parameter CA-9(c):
Parameter CA-9(d):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:

Configuration Management

CM-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] configuration management policy that:

    (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

CM-1 Control Summary Information
Responsible Role:
Parameter CM-1(a):
Parameter CM-1(a)(1):
Parameter CM-1(b):
Parameter CM-1(c)(1)-1:
Parameter CM-1(c)(1)-2:
Parameter CM-1(c)(2)-1:
Parameter CM-1(c)(2)-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)

CM-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [FedRAMP Assignment: at least annually and when a significant change occurs];
2. When required due to [FedRAMP Assignment: to include when directed by the JAB]; and
3. When system components are installed or upgraded.

CM-2 Additional FedRAMP Requirements and Guidance:

(b) (1) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

CM-2 Control Summary Information
Responsible Role:
Parameter CM-2(b)(1):

Parameter CM-2(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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
Part a:
Part b:

CM-4 Impact Analyses (L)(M)(H)

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

CM-4 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

CM-4 What is the solution and how is it implemented?

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

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

CM-5 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

CM-5 What is the solution and how is it implemented?

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

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

CM-6 Additional FedRAMP Requirements and Guidance:

Guidance: Compliance checks are used to evaluate configuration settings and provide general insight into the overall effectiveness of configuration management activities. CSPs and 3PAOs typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a per-control basis, where risks exist. Therefore, 3PAOs must also analyze compliance check findings as part of the controls assessment. Where a direct mapping exists, the 3PAO must document additional findings per control in the corresponding SAR Risk Exposure Table (RET), which are then documented in the CSP's Plan of Action and Milestones (POA&M). This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding, which is acceptable.

During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests.

(a) Requirement 1: The service provider shall use the DoD STIGs or Center for Internet Security guidelines to establish configuration settings.

(a) Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).

CM-6 Control Summary Information
Responsible Role:
Parameter CM-6(a):
Parameter CM-6(c)-1:
Parameter CM-6(c)-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

CM-6 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

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

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

CM-7 Additional FedRAMP Requirements and Guidance:

(b) Requirement: The service provider shall use Security guidelines (See CM-6) 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 STIGs or CIS is not available.

CM-7 Control Summary Information

Responsible Role:
Parameter CM-7(a):
Parameter CM-7(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the 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:
Parameter CM-8(a)(5):
Parameter CM-8(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation

☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document 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:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

CM-11 User-installed Software (L)(M)(H)

a. Establish [Assignment: organization-defined policies] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and

c. Monitor policy compliance [FedRAMP Assignment: Continuously (via CM-7 (5))].

CM-11 Control Summary Information
Responsible Role:
Parameter CM-11(a):
Parameter CM-11(b):
Parameter CM-11(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:
Part c:

Contingency Planning

CP-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] contingency planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

CP-1 Control Summary Information
Responsible Role:
Parameter CP-1(a):
Parameter CP-1(a)(1):
Parameter CP-1(b):
Parameter CP-1(c)(1)-1:
Parameter CP-1(c)(1)-2:
Parameter CP-1(c)(2)-1:
Parameter CP-1(c)(2)-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:
Part b:
Part c:

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

a. Develop a contingency plan for the system that:

1. Identifies essential mission and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and

7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [FedRAMP Assignment: at least annually];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect 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.

Requirement: CSPs must use the FedRAMP Information System Contingency Plan (ISCP) Template (available on the fedramp.gov: https://www.fedramp.gov/assets/resources/templates/SSP-Appendix-G-Information-System-Contingency-Plan-(ISCP)-Template.docx).

CP-2 Control Summary Information
Responsible Role:
Parameter CP-2(a)(7):
Parameter CP-2(b):

Parameter CP-2(d):
Parameter CP-2(f):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

Part d:
Part e:
Part f:
Part g:
Part h:

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

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within [FedRAMP Assignment: *See Additional Requirements] of assuming a contingency role or responsibility;

2. When required by system changes; and

3. [FedRAMP Assignment: at least annually] thereafter; and

b. Review and update contingency training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events].

CP-3 Additional FedRAMP Requirements and Guidance:

(a) Requirement: Privileged admins and engineers must take the basic contingency training within 10 days. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level. Newly hired critical contingency personnel must take this more in-depth training within 60 days of hire date when the training will have more impact.

CP-3 Control Summary Information
Responsible Role:

Parameter CP-3(a)(1):
Parameter CP-3(a)(3):
Parameter CP-3(b)-1:
Parameter CP-3(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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
Part a:

Part b:

CP-4 Contingency Plan Testing (L)(M)(H)

a. Test the contingency plan for the system [FedRAMP Assignment: at least every 3 years] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [FedRAMP Assignment: classroom exercise/tabletop written tests].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

CP-4 Additional FedRAMP Requirements and Guidance:

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

(b) Requirement: The service provider must include the Contingency Plan test results with the security package within the Contingency Plan-designated appendix (Appendix G, Contingency Plan Test Report).

CP-4 Control Summary Information
Responsible Role:
Parameter CP-4(a)-1:
Parameter CP-4(a)-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

CP-4 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [FedRAMP Assignment: daily incremental; weekly full];

b. Conduct backups of system-level information contained in the system [FedRAMP Assignment: daily incremental; weekly full];

c. Conduct backups of system documentation, including security- and privacy-related documentation [FedRAMP Assignment: daily incremental; weekly full]; and

d. Protect the confidentiality, integrity, and availability of backup information.

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.

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

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

(c) 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) or provides an equivalent alternative.

CP-9 Control Summary Information
Responsible Role:
Parameter CP-9(a)-1:
Parameter CP-9(a)-2:
Parameter CP-9(b):
Parameter CP-9(c):
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:

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

Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

CP-10 Control Summary Information
Responsible Role:
Parameter CP-10:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

Identification and Authentication

IA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] identification and authentication policy that:

    (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

IA-1 Control Summary Information
Responsible Role:
Parameter IA-1(a):
Parameter IA-1(a)(1):
Parameter IA-1(b):
Parameter IA-1(c)(1)-1:
Parameter IA-1(c)(1)-2:
Parameter IA-1(c)(2)-1:
Parameter IA-1(c)(2)-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)

IA-1 What is the solution and how is it implemented?

Part a:
Part b:
Part c:

IA-2 Identification and Authentication (Organizational Users) (L)(M)(H)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

IA-2 Additional FedRAMP Requirements and Guidance:

Guidance: "Phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

Requirement: All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate.

Requirement: For all control enhancements that specify multifactor authentication, the implementation must adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B.

Requirement: Multi-factor authentication must be phishing-resistant.

IA-2 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

IA-2 What is the solution and how is it implemented?

IA-2(1) Multi-factor Authentication to Privileged Accounts (L)(M)(H)

Implement multi-factor authentication for access to privileged accounts.

IA-2 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

IA-2(1) 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

IA-2(1) What is the solution and how is it implemented?

IA-2(2) Multi-factor Authentication to Non-privileged Accounts (L)(M)(H)

Implement multi-factor authentication for access to non-privileged accounts.

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

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

IA-2(2) 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

IA-2(2) What is the solution and how is it implemented?

IA-2(8) Access to Accounts — Replay Resistant (L)(M)(H)

Implement replay-resistant authentication mechanisms for access to [Selection (one-or-more): privileged accounts; non-privileged accounts].

IA-2(8) Control Summary Information
Responsible Role:
Parameter IA-2(8):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

IA-2(12) Acceptance of PIV Credentials (L)(M)(H)

Accept and electronically verify Personal Identity Verification-compliant 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:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable

Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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

Manage system identifiers by:

a. Receiving authorization from [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years].

IA-4 Control Summary Information

Responsible Role:
Parameter IA-4(a):
Parameter IA-4(d):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

Part c:
Part d:

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

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

IA-5 Additional FedRAMP Requirements and Guidance:

Guidance: SP 800-63C Section 6.2.3 Encrypted Assertion requires that authentication assertions be encrypted when passed through third parties, such as a browser. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE).

Requirement: Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 1. Link https://pages.nist.gov/800-63-3

IA-5 Control Summary Information
Responsible Role:
Parameter IA-5(f)-1:
Parameter IA-5(f)-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

IA-5 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:
Part f:
Part g:
Part h:
Part i:

IA-5(1) Password-based Authentication (L)(M)(H)

For password-based authentication:

(a) Maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

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

Guidance: Note that (c) and (d) require the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13).

Requirement: Password policies must be compliant with NIST SP 800-63B for all memorized, lookup, out-of-band, or One-Time-Passwords (OTP). Password policies shall not enforce special character or minimum password rotation requirements for memorized secrets of users.

(h) Requirement: For cases where technology doesn’t allow multi-factor authentication, these rules should be enforced: must have a minimum length of 14 characters and must support all printable ASCII characters.

For emergency use accounts, these rules should be enforced: must have a minimum length of 14 characters, must support all printable ASCII characters, and passwords must be changed if used.

IA-5(1) Control Summary Information
Responsible Role:
Parameter IA-5(1)(a):
Parameter IA-5(1)(h):
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:
Part f:

Part g:
Part h:

IA-6 Authentication Feedback (L)(M)(H)

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

IA-6 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

IA-6 What is the solution and how is it implemented?

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

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

IA-7 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

IA-7 What is the solution and how is it implemented?

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

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

IA-8 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

IA-8 What is the solution and how is it implemented?

IA-8(1) Acceptance of PIV Credentials from Other Agencies (L)(M)(H)

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

IA-8(1) 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

IA-8(1) What is the solution and how is it implemented?

IA-8(2) Acceptance of External Authenticators (L)(M)(H)

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

IA-8(2) 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

IA-8(2) What is the solution and how is it implemented?
Part a:
Part b:

IA-8(4) Use of Defined Profiles (L)(M)(H)

Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].

IA-8(4) Control Summary Information
Responsible Role:

Parameter IA-8(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

IA-8(4) What is the solution and how is it implemented?

IA-11 Re-authentication (L)(M)(H)

Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

IA-11 Additional FedRAMP Requirements and Guidance:

Guidance: The fixed time period cannot exceed the limits set in SP 800-63. At this time, they are:

- AAL1 (low baseline)
    - 30 days of extended session
    - No limit on inactivity.

IA-11 Control Summary Information
Responsible Role:
Parameter IA-11:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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-11 What is the solution and how is it implemented?

Incident Response

IR-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] incident response policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

IR-1 Control Summary Information
Responsible Role:
Parameter IR-1(a):
Parameter IR-1(a)(1):
Parameter IR-1(b):
Parameter IR-1(c)(1)-1:
Parameter IR-1(c)(1)-2:
Parameter IR-1(c)(2)-1:
Parameter IR-1(c)(2)-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)

IR-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

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

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

    1. Within [FedRAMP Assignment: ten (10) days for privileged users, thirty (30) days for Incident Response roles] of assuming an incident response role or responsibility or acquiring system access;

    2. When required by system changes; and

    3. [FedRAMP Assignment: at least annually] thereafter; and

b. Review and update incident response training content [FedRAMP Assignment: at least annually] and following [Assignment: organization-defined events].

IR-2 Control Summary Information
Responsible Role:
Parameter IR-2(a)(1):

Parameter IR-2(a)(3):
Parameter IR-2(b)-1:
Parameter IR-2(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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The FISMA definition of "incident" shall be used: "An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

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:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned

☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:

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

Track and document incidents.

IR-5 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

IR-5 What is the solution and how is it implemented?

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

a. Require personnel to report suspected incidents to the organizational incident response capability within [FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]; and

b. Report incident information to [Assignment: organization-defined authorities].

IR-6 Additional FedRAMP Requirements and Guidance:

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

IR-6 Control Summary Information
Responsible Role:
Parameter IR-6(a):
Parameter IR-6(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

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

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

IR-7 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

IR-7 What is the solution and how is it implemented?

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

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [FedRAMP Assignment: at least annually]; and
10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].

b. Distribute copies of the incident response plan to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

IR-8 Additional FedRAMP Requirements and Guidance:

(b) 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.

(d) 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.

IR-8 Control Summary Information
Responsible Role:
Parameter IR-8(a)(9)-1:

Parameter IR-8(a)(9)-2:
Parameter IR-8(a)(10):
Parameter IR-8(b):
Parameter IR-8(d):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:

Part b:
Part c:
Part d:
Part e:

Maintenance

MA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] maintenance policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

   1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

MA-1 Control Summary Information
Responsible Role:
Parameter MA-1(a):
Parameter MA-1(a)(1):
Parameter MA-1(b):
Parameter MA-1(c)(1)-1:
Parameter MA-1(c)(1)-2:
Parameter MA-1(c)(2)-1:
Parameter MA-1(c)(2)-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)

MA-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

MA-2 Controlled Maintenance (L)(M)(H)

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].

MA-2 Control Summary Information
Responsible Role:

Parameter MA-2(c):
Parameter MA-2(d):
Parameter MA-2(f):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

MA-2 What is the solution and how is it implemented?
Part a:
Part b:

Part c:
Part d:
Part e:
Part f:

MA-4 Nonlocal Maintenance (L)(M)(H)

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

MA-4 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

MA-4 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:

MA-5 Maintenance Personnel (L)(M)(H)

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-5 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

MA-5 What is the solution and how is it implemented?

Part a:
Part b:
Part c:

Media Protection

MP-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] media protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

   1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

MP-1 Control Summary Information
Responsible Role:
Parameter MP-1(a):
Parameter MP-1(a)(1):
Parameter MP-1(b):
Parameter MP-1(c)(1)-1:
Parameter MP-1(c)(1)-2:
Parameter MP-1(c)(2)-1:
Parameter MP-1(c)(2)-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:
Part b:
Part c:

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

Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

MP-2 Control Summary Information
Responsible Role:
Parameter MP-2-1:
Parameter MP-2-2:
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

MP-2 What is the solution and how is it implemented?

MP-6 Media Sanitization (L)(M)(H)

a. Sanitize [FedRAMP Assignment: techniques and procedures IAW NIST SP 800-88 Section 4: Reuse and Disposal of Storage Media and Hardware] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-6 Control Summary Information
Responsible Role:
Parameter MP-6(a)-1:
Parameter MP-6(a)-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

MP-6 What is the solution and how is it implemented?
Part a:
Part b:

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

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

MP-7 Control Summary Information
Responsible Role:
Parameter MP-7(a)-1:
Parameter MP-7(a)-2:
Parameter MP-7(a)-3:
Parameter MP-7(a)-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?
Part a:
Part b:

Physical and Environmental Protection

PE-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

PE-1 Control Summary Information
Responsible Role:
Parameter PE-1(a):
Parameter PE-1(a)(1):
Parameter PE-1(b):
Parameter PE-1(c)(1)-1:
Parameter PE-1(c)(1)-2:
Parameter PE-1(c)(2)-1:
Parameter PE-1(c)(2)-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)

PE-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PE-2 Physical Access Authorizations (L)(M)(H)

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least annually]; and

d. Remove individuals from the facility access list when access is no longer required.

PE-2 Control Summary Information
Responsible Role:
Parameter PE-2(c):
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

PE-3 Physical Access Control (L)(M)(H)

a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];

b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];

d. Escort visitors and control visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [FedRAMP Assignment: at least annually] every [Assignment: organization-defined frequency]; and

g. Change combinations and keys [FedRAMP Assignment: at least annually] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

PE-3 Control Summary Information
Responsible Role:
Parameter PE-3(a):
Parameter PE-3(a)(2):
Parameter PE-3(b):

Parameter PE-3(c):
Parameter PE-3(d):
Parameter PE-3(f)-1:
Parameter PE-3(f)-2:
Parameter PE-3(g):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-3 What is the solution and how is it implemented?

Part a:
Part b:
Part c:
Part d:
Part e:
Part f:
Part g:

PE-6 Monitoring Physical Access (L)(M)(H)

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [FedRAMP Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

PE-6 Control Summary Information
Responsible Role:
Parameter PE-6(b)-1:
Parameter PE-6(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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-6 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PE-8 Visitor Access Records (L)(M)(H)

a. Maintain visitor access records to the facility where the system resides for [FedRAMP Assignment: for a minimum of one (1) year];

b. Review visitor access records [FedRAMP Assignment: at least monthly]; and

c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

PE-8 Control Summary Information
Responsible Role:
Parameter PE-8(a):
Parameter PE-8(b):
Parameter PE-8(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-8 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PE-12 Emergency Lighting (L)(M)(H)

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-12 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

PE-12 What is the solution and how is it implemented?

PE-13 Fire Protection (L)(M)(H)

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

PE-13 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

PE-13 What is the solution and how is it implemented?

PE-14 Environmental Controls (L)(M)(H)

a. Maintain [FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and

b. Monitor environmental control levels [FedRAMP Assignment: continuously].

PE-14 Additional FedRAMP Requirements and Guidance:

(a) Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

PE-14 Control Summary Information
Responsible Role:
Parameter PE-14(a)-1:
Parameter PE-14(a)-2:
Parameter PE-14(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PE-14 What is the solution and how is it implemented?

Part a:
Part b:

PE-15 Water Damage Protection (L)(M)(H)

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-15 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

PE-15 What is the solution and how is it implemented?

PE-16 Delivery and Removal (L)(M)(H)

a. Authorize and control [FedRAMP Assignment: all information system components] entering and exiting the facility; and

b. Maintain records of the system components.

PE-16 Control Summary Information
Responsible Role:
Parameter PE-16(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

PE-16 What is the solution and how is it implemented?
Part a:
Part b:

Planning

PL-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

PL-1 Control Summary Information
Responsible Role:
Parameter PL-1(a):
Parameter PL-1(a)(1):
Parameter PL-1(b):
Parameter PL-1(c)(1)-1:
Parameter PL-1(c)(1)-2:
Parameter PL-1(c)(2)-1:
Parameter PL-1(c)(2)-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:
Part b:
Part c:

PL-2 System Security and Privacy Plans (L)(M)(H)

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization’s enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];

c. Review the plans [FedRAMP Assignment: at least annually];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

PL-2 Control Summary Information
Responsible Role:
Parameter PL-2(a)(14):
Parameter PL-2(b):

Parameter PL-2(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:

Part e:

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

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented 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 system;

c. Review and update the rules of behavior [FedRAMP Assignment: at least every 3 years]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [FedRAMP Assignment: at least annually and when the rules are revised or changed].

PL-4 Control Summary Information
Responsible Role:
Parameter PL-4(c):
Parameter PL-4(d):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:
Part c:
Part d:

PL-4(1) Social Media and External Site/Application Usage Restrictions (L)(M)(H)

Include in the rules of behavior, restrictions on:

(a) Use of social media, social networking sites, and external sites/applications;

(b) Posting organizational information on public websites; and

(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

PL-4(1) 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

PL-4(1) What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PL-8 Security and Privacy Architectures (L)(M)(H)

a. Develop security and privacy architectures for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
3. Describe how the architectures are integrated into and support the enterprise architecture; and
4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [FedRAMP Assignment: at least annually and when a significant change occurs] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-8 Additional FedRAMP Requirements and Guidance:

(b) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

PL-8 Control Summary Information
Responsible Role:
Parameter PL-8(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented

☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

PL-10 Baseline Selection (L)(M)(H)

Select a control baseline for the system.

PL-10 Additional FedRAMP Requirements and Guidance:

Requirement: Select the appropriate FedRAMP Baseline.

PL-10 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

PL-10 What is the solution and how is it implemented?

PL-11 Baseline Tailoring (L)(M)(H)

Tailor the selected control baseline by applying specified tailoring actions.

PL-11 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

PL-11 What is the solution and how is it implemented?

Personnel Security

PS-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] personnel security policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

PS-1 Control Summary Information
Responsible Role:

Parameter PS-1(a):
Parameter PS-1(a)(1):
Parameter PS-1(b):
Parameter PS-1(c)(1)-1:
Parameter PS-1(c)(1)-2:
Parameter PS-1(c)(2)-1:
Parameter PS-1(c)(2)-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)

PS-1 What is the solution and how is it implemented?
Part a:
Part b:

Part c:

PS-2 Position Risk Designation (L)(M)(H)

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [FedRAMP Assignment: at least every three years].

PS-2 Control Summary Information
Responsible Role:
Parameter PS-2(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PS-3 Personnel Screening (L)(M)(H)

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [FedRAMP Assignment: for national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low-risk positions].

PS-3 Control Summary Information
Responsible Role:
Parameter PS-3(b):
Implementation Status (check all that apply): ☐ Implemented

☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-3 What is the solution and how is it implemented?
Part a:
Part b:

PS-4 Personnel Termination (L)(M)(H)

Upon termination of individual employment:

a. Disable system access within [FedRAMP Assignment: four (4) hours];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-4 Control Summary Information
Responsible Role:
Parameter PS-4(a):
Parameter PS-4(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility)

☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-4 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:

PS-5 Personnel Transfer (L)(M)(H)

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [FedRAMP Assignment: twenty-four (24) hours];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [Assignment: organization-defined personnel or roles] within [FedRAMP Assignment: twenty-four (24) hours].

PS-5 Control Summary Information
Responsible Role:

Parameter PS-5(b)-1:
Parameter PS-5(b)-2:
Parameter PS-5(d)-1:
Parameter PS-5(d)-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

PS-5 What is the solution and how is it implemented?
Part a:

Part b:
Part c:
Part d:

PS-6 Access Agreements (L)(M)(H)

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [FedRAMP Assignment: at least annually]; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [FedRAMP Assignment: at least annually and any time there is a change to the user's level of access].

PS-6 Control Summary Information
Responsible Role:
Parameter PS-6(b):
Parameter PS-6(c)(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

PS-6 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

PS-7 External Personnel Security (L)(M)(H)

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [FedRAMP Assignment: including access control personnel responsible for the system and/or facilities, as appropriate] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [FedRAMP Assignment: within twenty-four (24) hours]; and

e. Monitor provider compliance with personnel security requirements.

PS-7 Control Summary Information
Responsible Role:
Parameter PS-7(d)-1:
Parameter PS-7(d)-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

PS-7 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:

PS-8 Personnel Sanctions (L)(M)(H)

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-8 Control Summary Information
Responsible Role:
Parameter PS-8(b)-1:
Parameter PS-8(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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

PS-8 What is the solution and how is it implemented?
Part a:
Part b:

PS-9 Position Descriptions (L)(M)(H)

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

PS-9 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

PS-9 What is the solution and how is it implemented?

Risk Assessment

RA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] risk assessment policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

RA-1 Control Summary Information
Responsible Role:
Parameter RA-1(a):
Parameter RA-1(a)(1):

Parameter RA-1(b):
Parameter RA-1(c)(1)-1:
Parameter RA-1(c)(1)-2:
Parameter RA-1(c)(2)-1:
Parameter RA-1(c)(2)-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)

RA-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

RA-2 Security Categorization (L)(M)(H)

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-2 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

RA-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

RA-3 Risk Assessment (L)(M)(H)

a. Conduct a risk assessment, including:

   1. Identifying threats to and vulnerabilities in the system;

   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [FedRAMP Assignment: security assessment report];

d. Review risk assessment results [FedRAMP Assignment: at least every three (3) years and when a significant change occurs];

e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and

f. Update the risk assessment [FedRAMP Assignment: at least every three (3) years] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

(e) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-3 Control Summary Information
Responsible Role:
Parameter RA-3(c):
Parameter RA-3(d):
Parameter RA-3(e):
Parameter RA-3(f):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:
Part f:

RA-3(1) Supply Chain Risk Assessment (L)(M)(H)

(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and

(b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in supply chain.

RA-3(1) Control Summary Information

Responsible Role:
Parameter RA-3(1)(a):
Parameter RA-3(1)(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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(1) What is the solution and how is it implemented?
Part a:
Part b:

RA-5 Vulnerability Monitoring and Scanning (L)(M)(H)

a. Monitor and scan for vulnerabilities in the system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications (including APIs) and databases] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures; and

3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate 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;

e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5 Additional FedRAMP Requirements and Guidance:

Guidance: See the FedRAMP Documents page, Vulnerability Scanning Requirements https://www.FedRAMP.gov/documents/.

Guidance: Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity and for FedRAMP does not require an entry onto the POA&M or entry onto the RET during any assessment phase.

Warning findings, on the other hand, are given a risk rating (low, moderate, high, or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment, or any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form.

Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a “warning” as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment, or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on “Tracking of Compliance Scans” in FAQs.

(a) Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

(d) Requirement: If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) the KEV remediation date supersedes the FedRAMP parameter requirement.

(e) Requirement: To include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-5 Control Summary Information
Responsible Role:
Parameter RA-5(a):
Parameter RA-5(d):

Parameter RA-5(e):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:

Part e:
Part f:

RA-5(2) Update Vulnerabilities to Be Scanned (L)(M)(H)

Update the system vulnerabilities to be scanned [FedRAMP Assignment: prior to a new scan].

RA-5(2) Control Summary Information
Responsible Role:
Parameter RA-5(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

RA-5(2) What is the solution and how is it implemented?

RA-5(11) Public Disclosure Program (L)(M)(H)

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-5(11) 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

RA-5(11) What is the solution and how is it implemented?

RA-7 Risk Response (L)(M)(H)

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-7 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

RA-7 What is the solution and how is it implemented?

System and Services Acquisition

SA-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and services acquisition policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

   1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SA-1 Control Summary Information
Responsible Role:
Parameter SA-1(a):
Parameter SA-1(a)(1):
Parameter SA-1(b):
Parameter SA-1(c)(1)-1:
Parameter SA-1(c)(1)-2:
Parameter SA-1(c)(2)-1:
Parameter SA-1(c)(2)-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)

SA-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SA-2 Allocation of Resources (L)(M)(H)

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-2 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

SA-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SA-3 System Development Life Cycle (L)(M)(H)

a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

SA-3 Control Summary Information
Responsible Role:
Parameter SA-3(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

SA-3 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

SA-4 Acquisition Process (L)(M)(H)

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one-or-more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

SA-4 Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.

See https://www.niap-ccevs.org/Product/index.cfm or https://www.commoncriteriaportal.org/products/.

Requirement: The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process).

SA-4 Control Summary Information
Responsible Role:
Parameter SA-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
SA-4 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:
Part e:
Part f:
Part g:
Part h:
Part i:

SA-4(10) Use of Approved PIV Products (L)(M)(H)

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

SA-4(10) 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

SA-4(10) What is the solution and how is it implemented?

SA-5 System Documentation (L)(M)(H)

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security and privacy functions and mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

   1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

   3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and

d. Distribute documentation to [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)].

SA-5 Control Summary Information
Responsible Role:
Parameter SA-5(c):
Parameter SA-5(d):

Implementation Status (check all that apply):

☐ Implemented

☐ Partially Implemented

☐ Planned

☐ Alternative implementation

☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:
Part c:
Part d:

SA-8 Security and Privacy Engineering Principles (L)(M)(H)

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].

SA-8 Control Summary Information
Responsible Role:
Parameter SA-8:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

SA-9 External System Services (L)(M)(H)

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [FedRAMP Assignment: Appropriate FedRAMP Security Controls Baseline (s) if Federal information is processed or stored within the external system];

b. Define and document organizational oversight and user roles and responsibilities regarding external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored].

SA-9 Control Summary Information
Responsible Role:
Parameter SA-9(a):
Parameter SA-9(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation

☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:

SA-22 Unsupported System Components (L)(M)(H)

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one-or-more): in-house support; [Assignment: organization-defined support from external providers]].

SA-22 Control Summary Information
Responsible Role:
Parameter SA-22(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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-22 What is the solution and how is it implemented?
Part a:
Part b:

System and Communications Protection

SC-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

  1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and communications protection policy that:

    (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

  2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

  1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

  2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SC-1 Control Summary Information
Responsible Role:
Parameter SC-1(a):

Parameter SC-1(a)(1):
Parameter SC-1(b):
Parameter SC-1(c)(1)-1:
Parameter SC-1(c)(1)-2:
Parameter SC-1(c)(2)-1:
Parameter SC-1(c)(2)-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)

SC-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SC-5 Denial-of-service Protection (L)(M)(H)

a. [FedRAMP Assignment: Protect against] the effects of the following types of denial-of-service events: [FedRAMP Assignment: at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack] and;

b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].

SC-5 Control Summary Information
Responsible Role:
Parameter SC-5(a)-1:
Parameter SC-5(a)-2:
Parameter SC-5(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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?
Part a:
Part b:

SC-7 Boundary Protection (L)(M)(H)

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are [Selection: Assignment: physically; logically] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

SC-7 Additional FedRAMP Requirements and Guidance:

(b) Guidance: SC-7 (b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs, and are specifically required to satisfy SC-7 part b and other controls. See the FedRAMP Subnets White Paper (https://www.fedramp.gov/assets/resources/documents/FedRAMP_subnets_white_paper.pdf) for additional information.

SC-7 Control Summary Information
Responsible Role:
Parameter SC-7(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:

Part c:

SC-8 Transmission Confidentiality and Integrity (L)(M)(H)

Protect the [Selection (one-or-more): confidentiality; integrity] of transmitted information.

SC-8 Additional FedRAMP Requirements and Guidance:

Guidance: For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8 (1), physical means as specified in SC-8 (5), or in combination.

For clarity, this control applies to all data in transit. Examples include the following data flows:

- Crossing the system boundary
- Between compute instances - including containers
- From a compute instance to storage
- Replication between availability zones
- Transmission of backups to storage
- From a load balancer to a compute instance
- Flows from management tools required for their work – e.g. log collection, scanning, etc.

The following applies only when choosing SC-8 (5) in lieu of SC-8 (1).

FedRAMP-Defined Assignment / Selection Parameters

SC-8 (5)-1 [a hardened or alarmed carrier Protective Distribution System (PDS) when outside of Controlled Access Area (CAA)]

SC-8 (5)-2 [prevent unauthorized disclosure of information AND detect changes to information]

Guidance: SC-8 (5) applies when physical protection has been selected as the method to protect confidentiality and integrity. For physical protection, data in transit must be in either a Controlled Access Area (CAA), or a Hardened or alarmed PDS.

Hardened or alarmed PDS: Shall be as defined in SECTION X - CATEGORY 2 PDS INSTALLATION GUIDANCE of CNSSI No.7003, titled PROTECTED DISTRIBUTION SYSTEMS (PDS). Per the CNSSI No. 7003 Section VIII, PDS must originate and terminate in a Controlled Access Area (CAA).

Controlled Access Area (CAA): Data will be considered physically protected, and in a CAA if it meets Section 2.3 of the DHS's Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. CSPs can meet Section 2.3 of the DHS' recommended practice by satisfactory implementation of the following controls PE-2 (1), PE-2 (2), PE-2 (3), PE-3 (2), PE-3 (3), PE-6 (2), and PE-6 (3). Note: When selecting SC-8 (5), the above SC-8(5), and the above referenced PE controls must be added to the SSP. CNSSI No.7003 can be accessed here: https://www.dcsa.mil/Portals/91/documents/ctp/nao/CNSSI_7003_PDS_September_2015.pdf. DHS Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies can be accessed here: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf.

SC-8 Control Summary Information
Responsible Role:
Parameter SC-8:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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?

SC-8(1) Cryptographic Protection (L)(M)(H)

Implement cryptographic mechanisms to [Selection (one-or-more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

Guidance: See M-22-09, including "Agencies encrypt all DNS requests and HTTP traffic within their environment." SC-8 (1) applies when encryption has been selected as the method to protect confidentiality and integrity. Otherwise refer to SC-8 (5). SC-8 (1) is strongly encouraged.

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13).

Guidance: When leveraging encryption from the underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Requirement: Please ensure SSP Section 10.3 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) is fully populated for reference in this control.

SC-8(1) Control Summary Information
Responsible Role:
Parameter SC-8(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

SC-8(1) What is the solution and how is it implemented?

SC-12 Cryptographic Key Establishment and Management (L)(M)(H)

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [FedRAMP Assignment: In accordance with Federal requirements].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: See references in NIST 800-53 documentation.

Guidance: Must meet applicable Federal Cryptographic Requirements. See References Section of control.

Guidance: Wildcard certificates may be used internally within the system but are not permitted for external customer access to the system.

SC-12 Control Summary Information
Responsible Role:
Parameter SC-12:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation

☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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?

SC-13 Cryptographic Protection (L)(M)(H)

a. Determine the [Assignment: organization-defined cryptographic uses]; and

b. Implement the following types of cryptography required for each specified cryptographic use: [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography].

SC-13 Additional FedRAMP Requirements and Guidance:

Guidance: This control applies to all use of cryptography. In addition to encryption, this includes functions such as hashing, random number generation, and key generation. Examples include the following:

- Encryption of data
- Decryption of data

- Generation of one-time passwords (OTPs) for MFA
- Protocols such as TLS, SSH, and HTTPS

The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP) https://csrc.nist.gov/projects/cryptographic-module-validation-program.

Guidance: For NSA-approved cryptography, the National Information Assurance Partnership (NIAP) oversees a national program to evaluate Commercial IT Products for Use in National Security Systems. The NIAP Product Compliant List can be found at the following location: https://www.niap-ccevs.org/Product/index.cfm.

Guidance: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Guidance: Moving to non-FIPS CM or product is acceptable when:

- FIPS validated version has a known vulnerability
- Feature with vulnerability is in use
- Non-FIPS version fixes the vulnerability
- Non-FIPS version is submitted to NIST for FIPS validation
- POA&M is added to track approval, and deployment when ready

Guidance: At a minimum, this control applies to cryptography in use for the following controls: AU-9(3), CP-9(8), IA-2(6), IA-5(1), MP-5, SC-8(1), and SC-28(1).

SC-13 Control Summary Information
Responsible Role:
Parameter SC-13(a):
Parameter SC-13(b):

Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
Part a:
Part b:

SC-15 Collaborative Computing Devices and Applications (L)(M)(H)

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [FedRAMP Assignment: no exceptions for computing devices]; and

b. Provide 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:
Parameter SC-15(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

SC-15 What is the solution and how is it implemented?
Part a:
Part b:

SC-20 Secure Name/Address Resolution Service (Authoritative Source) (L)(M)(H)

a. Provide 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

b. Provide 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 Additional FedRAMP Requirements and Guidance:

Guidance: SC-20 applies to use of external authoritative DNS to access a CSO from outside the boundary.

Guidance: External authoritative DNS servers may be located outside an authorized environment. Positioning these servers inside an authorized boundary is encouraged.

Guidance: CSPs are recommended to self-check DNSSEC configuration through one of many available analyzers such as Sandia National Labs (https://dnsviz.net).

Requirement: Control Description should include how DNSSEC is implemented on authoritative DNS servers to supply valid responses to external DNSSEC requests.

SC-20 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-20 What is the solution and how is it implemented?
Part a:

Part b:

SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (L)(M)(H)

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-21 Additional FedRAMP Requirements and Guidance:

Guidance: Accepting an unsigned reply is acceptable

Guidance: SC-21 applies to use of internal recursive DNS to access a domain outside the boundary by a component inside the boundary. DNSSEC resolution to access a component inside the boundary is excluded.

Requirement: Control description should include how DNSSEC is implemented on recursive DNS servers to make DNSSEC requests when resolving DNS requests from internal components to domains external to the CSO boundary.

- If the reply is signed, and fails DNSSEC, do not use the reply.
- If the reply is unsigned, CSP chooses the policy to apply.

Requirement: Internal recursive DNS servers must be located inside an authorized environment. It is typically within the boundary, or leveraged from an underlying IaaS/PaaS.

SC-21 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-21 What is the solution and how is it implemented?

SC-22 Architecture and Provisioning for Name/Address Resolution Service (L)(M)(H)

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

SC-22 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-22 What is the solution and how is it implemented?

SC-28 Protection of Information at Rest (L)(M)(H)

Protect the [Selection (one-or-more): confidentiality/integrity] of the following information at rest: [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.

Guidance: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Guidance: Note that this enhancement requires the use of cryptography in accordance with SC-13.

SC-28 Control Summary Information
Responsible Role:
Parameter SC-28-1:
Parameter SC-28-2:
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-28 What is the solution and how is it implemented?

SC-28(1) Cryptographic Protection (L)(M)(H)

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [FedRAMP Assignment: all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels]: [Assignment: organization-defined information].

SC-28 (1) Additional FedRAMP Requirements and Guidance:

Guidance: Organizations should select a mode of protection that is targeted towards the relevant threat scenarios.

Examples:

A. Organizations may apply full disk encryption (FDE) to a mobile device where the primary threat is loss of the device while storage is locked.

B. For a database application housing data for a single customer, encryption at the file system level would often provide more protection than FDE against the more likely threat of an intruder on the operating system accessing the storage.

C. For a database application housing data for multiple customers, encryption with unique keys for each customer at the database record level may be more appropriate.

SC-28(1) Control Summary Information

Responsible Role:
Parameter SC-28(1)-1:
Parameter SC-28(1)-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-28(1) What is the solution and how is it implemented?

SC-39 Process Isolation (L)(M)(H)

Maintain a separate execution domain for each executing system process.

SC-39 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-39 What is the solution and how is it implemented?

System and Information Integrity

SI-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

   1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and information integrity policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

   1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

   2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SI-1 Control Summary Information

Responsible Role:
Parameter SI-1(a):
Parameter SI-1(a)(1):
Parameter SI-1(b):
Parameter SI-1(c)(1)-1:
Parameter SI-1(c)(1)-2:
Parameter SI-1(c)(2)-1:
Parameter SI-1(c)(2)-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)

SI-1 What is the solution and how is it implemented?
Part a:

Part b:
Part c:

SI-2 Flaw Remediation (L)(M)(H)

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [FedRAMP Assignment: within thirty (30) days of release of updates] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

SI-2 Control Summary Information
Responsible Role:
Parameter SI-2(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (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:
Part b:
Part c:
Part d:

SI-3 Malicious Code Protection (L)(M)(H)

a. Implement [FedRAMP Assignment: signature based and non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints and network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [FedRAMP Assignment: to include blocking and quarantining malicious code] and send alert to [FedRAMP Assignment; administrator or defined security personnel near-real time] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-3 Control Summary Information
Responsible Role:
Parameter SI-3(a):
Parameter SI-3(c)(1)-1:
Parameter SI-3(c)(1)-2:
Parameter SI-3(c)(2)-1:
Parameter SI-3(c)(2)-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

SI-3 What is the solution and how is it implemented?
Part a:
Part b:
Part c:
Part d:

SI-4 System Monitoring (L)(M)(H)

a. Monitor the system to detect:

   1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and

   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

   1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined 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:
Parameter SI-4(a)(1):
Parameter SI-4(b):
Parameter SI-4(g)-1:
Parameter SI-4(g)-2:
Parameter SI-4(g)-3:
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation

☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:
Part e:
Part f:
Part g:

SI-5 Security Alerts, Advisories, and Directives (L)(M)(H)

a. Receive system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT and Cybersecurity and Infrastructure Security Agency (CISA) Directives] on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: [Selection (one-or-more): [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and

d. Implement security directives in accordance with established timeframes or notify the issuing organization of the degree of noncompliance.

SI-5 Additional FedRAMP Requirements and Guidance:

Requirement: Service Providers must address the CISA Emergency and Binding Operational Directives applicable to their cloud service offering per FedRAMP guidance. This includes listing the applicable directives and stating compliance status.

SI-5 Control Summary Information
Responsible Role:
Parameter SI-5(a):
Parameter SI-5(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation

☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:
Part b:
Part c:
Part d:

SI-12 Information Management and Retention (L)(M)(H)

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

SI-12 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

SI-12 What is the solution and how is it implemented?

Supply Chain Risk Management

SR-1 Policy and Procedures (L)(M)(H)

a. Develop, document, and disseminate to [FedRAMP Assignment: to include chief privacy and ISSO and/or similar role or designees]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] supply chain risk management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy [FedRAMP Assignment: at least every 3 years] and following [Assignment: organization-defined events]; and

2. Procedures [FedRAMP Assignment: at least annually] and following [FedRAMP Assignment: significant changes].

SR-1 Control Summary Information
Responsible Role:
Parameter SR-1(a):

Parameter SR-1(a)(1):
Parameter SR-1(b):
Parameter SR-1(c)(1)-1:
Parameter SR-1(c)(1)-2:
Parameter SR-1(c)(2)-1:
Parameter SR-1(c)(2)-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)

SR-1 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SR-2 Supply Chain Risk Management Plan (L)(M)(H)

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];

b. Review and update the supply chain risk management plan [FedRAMP Assignment: at least annually] or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2 Control Summary Information
Responsible Role:
Parameter SR-2(a):
Parameter SR-2(b):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific)

☐ Shared (Service Provider and Customer Responsibility)

☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-2 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SR-2(1) Establish SCRM Team (L)(M)(H)

Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].

SR-2(1) Control Summary Information
Responsible Role:
Parameter SR-2(1)-1:
Parameter SR-2(1)-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

SR-2(1) What is the solution and how is it implemented?

SR-3 Supply Chain Controls and Processes (L)(M)(H)

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and

c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan [Assignment: organization-defined document]].

SR-3 Additional FedRAMP Requirements and Guidance:

Requirement: CSO must document and maintain the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary.

SR-3 Control Summary Information
Responsible Role:
Parameter SR-3(a)-1:
Parameter SR-3(a)-2:
Parameter SR-3(b):
Parameter SR-3(c):
Implementation Status (check all that apply): ☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific)

☐ Shared (Service Provider and Customer Responsibility)

☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-3 What is the solution and how is it implemented?
Part a:
Part b:
Part c:

SR-5 Acquisition Strategies, Tools, and Methods (L)(M)(H)

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].

SR-5 Control Summary Information
Responsible Role:
Parameter SR-5:

Implementation Status (check all that apply):

☐ Implemented

☐ Partially Implemented

☐ Planned

☐ Alternative implementation

☐ Not Applicable

Control Origination (check all that apply):

☐ Service Provider Corporate

☐ Service Provider System Specific

☐ Service Provider Hybrid (Corporate and System Specific)

☐ Configured by Customer (Customer System Specific)

☐ Provided by Customer (Customer System Specific)

☐ Shared (Service Provider and Customer Responsibility)

☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-5 What is the solution and how is it implemented?

SR-8 Notification Agreements (L)(M)(H)

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [FedRAMP Assignment: notification of supply chain compromises and results of assessment or audits].

SR-8 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities.

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

SR-8 What is the solution and how is it implemented?

SR-10 Inspection of Systems or Components (L)(M)(H)

Inspect the following systems or system components [Selection (one-or-more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].

SR-10 Control Summary Information
Responsible Role:
Parameter SR-10-1:
Parameter SR-10-2:
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

SR-10 What is the solution and how is it implemented?

SR-11 Component Authenticity (L)(M)(H)

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to [Selection (one-or-more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

SR-11 Additional FedRAMP Requirements and Guidance:

Requirement: CSOs must ensure that their supply chain vendors provide authenticity of software and patches, and the vendor must have a plan to protect the development pipeline.

SR-11 Control Summary Information
Responsible Role:
Parameter SR-11(b):
Implementation Status (check all that apply):

☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

SR-11 What is the solution and how is it implemented?
Part a:
Part b:

SR-11(1) Anti-counterfeit Training (L)(M)(H)

Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

SR-11(1) Control Summary Information
Responsible Role:
Parameter SR-11(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

SR-11(1) What is the solution and how is it implemented?

SR-11(2) Configuration Control for Component Service and Repair (L)(M)(H)

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [FedRAMP Assignment: all].

SR-11(2) Control Summary Information
Responsible Role:
Parameter SR-11(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

SR-11(2) What is the solution and how is it implemented?

SR-12 Component Disposal (L)(M)(H)

Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].

SR-12 Control Summary Information
Responsible Role:
Parameter SR-12-1:
Parameter SR-12-2:
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

SR-12 What is the solution and how is it implemented?