nistBlue

FedRAMP System Security Plan (Template)



<CSP Name>

<Information System Name>

<CSP Version #.#>

<Date>

**Company Sensitive and Proprietary**

**For Authorized Use Only**

# System Security Plan

# Prepared by

| Identification of Organization that Prepared this Document | | |
| --- | --- | --- |
| <**insert logo**> | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

# Prepared for

| Identification of Cloud Service Provider | | |
| --- | --- | --- |
| <**insert logo**> | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

Template Revision History

| Date | Description | Version of System | Author |
| --- | --- | --- | --- |
| 6/6/2014 | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. | 2.0 | FedRAMP PMO |

Table of Contents

[System Security Plan 2](#_Toc389558027)

[Prepared by 2](#_Toc389558028)

[Prepared for 2](#_Toc389558029)

[About This Document 11](#_Toc389558030)

[System Security Plan Approvals 12](#_Toc389558031)

[1. Information System Name/Title 13](#_Toc389558032)

[2. Information System Categorization 13](#_Toc389558033)

[2.1. Information Types 14](#_Toc389558034)

[2.2. Security Objectives Categorization (FIPS 199) 16](#_Toc389558035)

[2.3. E-Authentication Determination 16](#_Toc389558036)

[3. Information System Owner 17](#_Toc389558037)

[4. Authorizing Official 18](#_Toc389558038)

[5. Other Designated Contacts 18](#_Toc389558039)

[6. Assignment of Security Responsibility 19](#_Toc389558040)

[7. Information System Operational Status 20](#_Toc389558041)

[8. Information System Type 21](#_Toc389558042)

[8.1. Cloud Service Models 21](#_Toc389558043)

[8.2. Cloud Deployment Models 22](#_Toc389558044)

[8.3. Leveraged Authorizations 23](#_Toc389558045)

[9. General System Description 23](#_Toc389558046)

[9.1. System Function or Purpose 23](#_Toc389558047)

[9.2. Information System Components and Boundaries 24](#_Toc389558048)

[9.3. Types of Users 24](#_Toc389558049)

[9.4. Network Architecture 25](#_Toc389558050)

[10. System Environment 26](#_Toc389558051)

[10.1. Hardware Inventory 26](#_Toc389558052)

[10.2. Software Inventory 27](#_Toc389558053)

[10.3. Network Inventory 28](#_Toc389558054)

[10.4. Data Flow 30](#_Toc389558055)

[10.5. Ports, Protocols and Services 30](#_Toc389558056)

[11. System Interconnections 32](#_Toc389558057)

[12. Applicable Laws and Regulations 33](#_Toc389558058)

[12.1. Applicable Laws 33](#_Toc389558059)

[12.2. Applicable Standards and Guidance 33](#_Toc389558060)

[13. Minimum Security Controls 34](#_Toc389558061)

[Access Control (AC) 44](#_Toc389558062)

[Awareness and Training (AT) 95](#_Toc389558063)

[Audit and Accountability (AU) 101](#_Toc389558064)

[Security Assessment and Authorization (CA) 124](#_Toc389558065)

[Configuration Management (CM) 145](#_Toc389558066)

[Contingency Planning (CP) 178](#_Toc389558067)

[Identification and Authentication (IA) 207](#_Toc389558068)

[Incident Response (IR) 238](#_Toc389558069)

[Maintenance (MA) 260](#_Toc389558070)

[Media Protection (MP) 274](#_Toc389558071)

[Physical and Environmental Protection (PE) 285](#_Toc389558072)

[Planning (PL) 309](#_Toc389558073)

[Personnel Security (PS) 318](#_Toc389558074)

[Risk Assessment (RA) 330](#_Toc389558075)

[System and Services Acquisition (SA) 343](#_Toc389558076)

[System and Communications Protection (SC) 373](#_Toc389558077)

[System and Information Integrity (SI) 409](#_Toc389558078)

[14. ATTACHMENT 1 - [Information Security Policies] 444](#_Toc389558079)

[15. ATTACHMENT 2 - [User Guide] 444](#_Toc389558080)

[16. ATTACHMENT 3 - [e-Authentication Worksheet] 444](#_Toc389558081)

[17. ATTACHMENT 4 - [PTA/PIA] 444](#_Toc389558082)

[18. ATTACHMENT 5 - [Rules of Behavior] 444](#_Toc389558083)

[19. ATTACHMENT 6 - [IT Contingency Plan] 444](#_Toc389558084)

[20. ATTACHMENT 7 - [Configuration Management Plan] 444](#_Toc389558085)

[21. ATTACHMENT 8 - [Incident Response Plan] 444](#_Toc389558086)

[22. ATTACHMENT 9 - [CIS Workbook] 444](#_Toc389558087)

List of Tables

[Table 1-1. Information System Name and Title 35](#_Toc388621429)

[Table 2- 1. Security Categorization 35](#_Toc388621430)

[Table 2- 2. Sensitivity Categorization of Information Types 38](#_Toc388621431)

[Table 2- 3. Security Impact Level 38](#_Toc388621432)

[Table 2- 4. Baseline Security Configuration 39](#_Toc388621433)

[Table 2- 5. E-Authentication Questions 39](#_Toc388621434)

[Table 2- 6. E-Authentication Level Determination 39](#_Toc388621435)

[Table 3- 1. Information System Owner 40](#_Toc388621436)

[Table 5- 1. Information System Management Point of Contact 41](#_Toc388621437)

[Table 5- 2. Information System Technical Point of Contact 41](#_Toc388621438)

[Table 6- 1. CSP Internal ISSO (or Equivalent) 42](#_Toc388621439)

[Table 6- 2. FedRAMP or Agency Appointed ISSO 42](#_Toc388621440)

[Table 7- 1. System Status 43](#_Toc388621441)

[Table 8- 1. Service Layers Represented in this SSP 43](#_Toc388621442)

[Table 8- 2. Cloud Deployment Model Represented in this SSP 43](#_Toc388621443)

[Table 8- 2. Leveraged Authorizations 43](#_Toc388621444)

[Table 9- 1. User Roles and Privileges 47](#_Toc388621445)

[Table 10- 1. Server Hardware Components 49](#_Toc388621446)

[Table 10- 2. Software Components 50](#_Toc388621447)

[Table 10- 3. Network Components 51](#_Toc388621448)

[Table 10- 4. Ports, Protocols, and Services 53](#_Toc388621449)

[Table 11- 1. System Interconnections 54](#_Toc388621450)

[Table 13- 1. Summary of Required Security Controls 63](#_Toc388621451)

[Table 13- 2. Authorized Connections 153](#_Toc388621452)

List of Figures

[Figure 10-1. Network Diagram 46](#_Toc383465519)

[Figure 10-2. Data Flow Diagram 50](#_Toc383465520)

# About This Document

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

The System Security Plan is the main document in which the CSP describes all the security controls in use on the information system and their implementation.

## Who should use this document?

This document is intended to be used by service providers who are applying for a Provisional Authorization through the U.S. Federal government FedRAMP program. U.S. Federal agencies may want to use it to document information systems security plans that are not part of the FedRAMP program.

Other uses of this template include using it to document organizational information security controls for the purpose of creating a plan to manage a large information security infrastructure. Complex and sophisticated systems are difficult to manage without a documented understanding of how the infrastructure is architected.

## How this document is organized

This document is divided into six sections and includes <**number**> attachments. Most sections include subsections.

|  |  |
| --- | --- |
| Section 1 | Identifies the system. |
| Section 2 | Describes the system categorization in accordance with FIPS 199. |
| Section 3 | Identifies the system owner and provides contact information. |
| Section 4 | Identifies the authorizing official. |
| Section 5 | Identifies other designated contacts. |
| Section 6 | Identifies the assignment of security responsibility. |
| Section 7 | Identifies the operational status of the information system. |
| Section 8 | Identifies the type of information system. |
| Section 9 | Describes the function and purpose of the information system. |
| Section 10 | Describes the information system environment. |
| Section 11 | Identifies interconnections between other information systems. |
| Section 12 | Describes laws and regulations related to operations of the information system. |
| Section 13 | Provides an in-depth description of how each security control is implemented. |

## How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact [*info@fedramp.gov*](mailto:info@fedramp.gov)

For more information about the FedRAMP project, see [www.fedramp.gov](http://www.fedramp.gov)

# System Security Plan Approvals

Cloud Service Provider Signatures

|  |
| --- |
|  |
| <**Name**> <**Date**>  <**Title**>  <**Cloud Service Provider**> |
|  |
| <**Name**> <**Date**>  <**Title**>  <**Cloud Service Provider**> |
|  |
| <**Name**> <**Date**>  <**Title**>  <**Cloud Service Provider**> |

1. Information System Name/Title

This System Security Plan provides an overview of the security requirements for the <**Information System Name**> (<**Information System Abbreviation>**) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the <**Information System Abbreviation>** information system.

**Note:** Once the name and abbreviation for the system and all the system’s components is established in this section, use the exact same name and abbreviation throughout the SSP.

The security safeguards implemented for the <**Information System Abbreviation**> system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Information System Name | Information System Abbreviation |
|  |  |  |

Table 1-1. Information System Name and Title

1. Information System Categorization

The overall information system sensitivity categorization is noted in the table that follows. The FIPS 199 document is attached in section <**SSP Section Number**>.

|  |  |
| --- | --- |
| Low |  |
| Moderate |  |
| High |  |

Table 2- 1. Security Categorization

* 1. Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from <**Information System Abbreviation**>. The selection of the information types is based on guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* which is based on NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The tables also identify the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is *low* if—

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

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is *moderate* if—

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

- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is *high* if—

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

- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

*Instruction: Categorize the information system in accordance with FIPS-199 and NIST SP 800-60. Transfer the information types in the table that follows. Record the sensitivity level determination for Confidentiality, Integrity, and Availability as High, Moderate, or Low. Add more rows as needed to add more information types. Use NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories, Volumes I & II, Revision 1 for guidance.*

*Controls must be implemented at the highest sensitivity level present on the system (high water-mark).For example if a system is Confidentiality “low”, Integrity “moderate”, and Availability “low”, all controls must be implemented as moderate.*

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| System Development | C.3.5.1 | Low | Moderate | Low |
|  |  |  |  |  |
|  |  |  |  |  |

Table 2- 2. Sensitivity Categorization of Information Types

* 1. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2, Information Types, for the <**Information System Abbreviation**> default to the high-water mark for the noted Information Types as identified in the table below.

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality |  |
| Integrity |  |
| Availability |  |

Table 2- 3. Security Impact Level

Through review and analysis it has been determined that the baseline security categorization for the <**Information System Abbreviation>** system is listed in the table that follows.

|  |  |
| --- | --- |
| <**Information System Abbreviation**> Security Categorization | Low, Moderate or High |

Table 2- 4. Baseline Security Configuration

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

* 1. E-Authentication Determination

The information system e-Authentication Determination is described in the table that follows. The e-Authentication document is attached in section <**SSP Section Number**>.

|  |  |  |
| --- | --- | --- |
| Yes | No | E-Authentication Question |
|  |  | Does the system require authentication via the Internet? |
|  |  | Is data being transmitted over the Internet via browsers? |
|  |  | Do users connect to the system from over the Internet? |

Table 2- 5. E-Authentication Questions

*Instruction: Any information system that has a “No” response to**any one of the three questions does not need an E-Authentication risk analysis or assessment.**For a system that has a "Yes" response to all of the questions, complete the E-Authentication Plan (a template is available).*

**Note:** Refer to *OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies* for more information on e-Authentication.

The summary E-Authentication Level is recorded in the table that follows.

| E-Authentication Determination | |
| --- | --- |
| System Name |  |
| System Owner |  |
| Assurance Level |  |
| Date Approved |  |

Table 2- 6. E-Authentication Level Determination

*Instruction: The Assurance Level in the table above, must be defined as follows:*

1. *Level 1: Little or no confidence in the asserted identity’s validity*
2. *Level 2: Some confidence in the asserted identity’s validity*
3. *Level 3: High confidence in the asserted identity’s validity*
4. *Level 4: Very high confidence in the asserted identity’s validity.*
5. Information System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Table 3- 1. Information System Owner

1. Authorizing Official

*Instruction: The Authorizing Official is determined by the path that the CSP is using to obtain an authorization.*

1. *JAB P-ATO: Federal Risk Authorization Management Program (FedRAMP), Joint Authorization Board (JAB) as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DOD) and Department of Homeland Security (DHS)*
2. *Agency ATO: Agency Authorizing Official Name, title and contact information.*
3. *CSP Supplied: Leave blank.*

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the <**Insert AO information as instructed above**>.

* 1. Other Designated Contacts

*Instruction: Authorizing officials should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. Authorizing officials should edit, add, modify the contacts in this section as they see fit.*

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Table 5- 1. Information System Management Point of Contact

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Table 5- 2. Information System Technical Point of Contact

*Instruction: Add more tables as needed.*

1. Assignment of Security Responsibility

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Table 6- 1. CSP Internal ISSO (or Equivalent)

|  |  |
| --- | --- |
| Name |  |
| Title | ISSO |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

Table 6- 2. AO ISSO

1. Information System Operational Status

The system is currently in the life-cycle phase noted in the table that follows. (Only operational systems can be granted an ATO).

| System Status | | |
| --- | --- | --- |
|  | Operational | The system is operating and in production. |
|  | Under Development | The system is being designed, developed, or implemented |
|  | Major Modification | The system is undergoing a major change, development, or transition. |
|  | Other | Explain: |

Table 7- 1. System Status

*Instruction: Select as many status indicators that apply. If more than one status is selected, list which components of the system are covered under each status indicator.*

1. Information System Type

The <**Information System Abbreviation**> makes use of unique managed service provider architecture layer(s).

* 1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. The layers of the <**Information System Abbreviation**> defined in this SSP are indicated in the table that follows.

*Instruction: Check all layers that apply.*

| Service Provider Architecture Layers | | |
| --- | --- | --- |
|  | Software as a Service (SaaS) | Major Application |
|  | Platform as a Service (PaaS) | Major Application |
|  | Infrastructure as a Service (IaaS) | General Support System |
|  | Other | Explain: |

Table 8- 1. Service Layers Represented in this SSP

**Note:** Refer to *NIST SP 800-145* for information on cloud computing architecture models.

* 1. Cloud Deployment Models

Information systems, particularly those based on cloud services and infrastructures, are made up of different deployment models. The deployment models of the <**Information System Abbreviation**> that are defined in this SSP, and are not leveraged by any other Provisional Authorizations, are indicated in the table that follows.

*Instruction: Check deployment model that applies.*

| Service Provider Cloud Deployment Model | | |
| --- | --- | --- |
|  | Public | Cloud services and infrastructure supporting multiple organizations and agency  clients |
|  | Private | Cloud services and infrastructure dedicated to a specific organization/agency and no other clients |
|  | Community | Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations |
|  | Hybrid | Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) |

Table 8- 2. Cloud Deployment Model Represented in this SSP

* 1. Leveraged Authorizations

*Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers, can be qualified in one System Security Plan.*

*See the section on Use Cases in Guide to Understanding FedRAMP for more information.*

*If a lower level layer has been granted an Authorization, and another higher level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows.*

The <**Information System Abbreviation**> <**plans to/does not plan to**> leverage a pre-existing Provisional Authorization. Provisional Authorizations leveraged by this <**Information System Abbreviation**> are noted in the table that follows.

| Information System Name | Service Provider Owner | Date Granted |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Table 8- 2. Leveraged Authorizations

1. General System Description

This section includes a general description of the <**Information System Abbreviation**>.

* 1. System Function or Purpose

*Instruction: In the space that follows, describe the purpose and functions of this system.*

* 1. Information System Components and Boundaries

*Instruction: In the space that follows, describe the information system’s major components, inter-connections, and boundaries in sufficient detail that accurately depicts the authorization boundary for the information system. Formal names of components as they are known at the service provider organization in functional specs, configuration guides, other documents, and live configurations shall be named here and described. Ensure that the discussion on boundaries is consistent with the network diagram shown in Section 9.4. See the Guide to Understanding FedRAMP for more information.*

* 1. Types of Users

All users have their employee status categorized with a sensitivity level in accordance with PS-2. Employees (or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows.

*Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles (whether or not they have logical access) including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators, and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)*

*This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.*

*The roles in this table establish the roles that will later be used in the controls in the Responsible Role parameter. Ensure that roles and privileges are specific and detailed enough to support 3PAO testing. Add additional rows if necessary.*

| Role | Internal or External | Sensitivity Level  (as determined by OPM guidance in FIN 10-06, Position Designation Requirements) | Authorized Privileges and Functions Performed |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 9- 1. User Roles and Privileges

There are currently <**number**> of internal users and <**number**> of external users. Within one year, it is anticipated that there will be <**number**> of internal users and <**number**> of external users.

* 1. Network Architecture

*Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, DNS servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, Internet connectivity providers, telecom circuit numbers, and network numbers/VLANs. Major security components should also be represented. If necessary, include multiple network diagrams.*

*Assessors should be able to easily map hardware, software, and network inventories back to this diagram.*

The following architectural diagram(s) provides a visual depiction of the system network components that constitute <**Information System Abbreviation**>.

<**insert diagram**>

Figure 10-1. Network Diagram

1. System Environment

*Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g. production environment, test environment, staging or QA environments. Include alternate, backup and operational facilities.*

* 1. Hardware Inventory

The following table lists the principal hardware components for <**Information System Abbreviation**>.

*Instruction: This is a comprehensive inventory of all system components.*

*The first three rows are sample entries. If service offerings do not include hardware because all hardware is leveraged from a pre-existing Provisional Authorization, write “None” in the first column. Add additional rows as needed.*

*The inventory can be included as an attachment.*

| Hostname | Make | Model and Firmware | Location | Components that Use this Device |
| --- | --- | --- | --- | --- |
| hostname1.com | Company | SilverEdge M710, 4.6ios | Dallas, Rm. 6, Rack 4 | AppOne, EAuthApp |
| hostname2.com | Company | SilverEdge M610, 4.6ios | Datacenter2, Rack 7 | VMs 1-50 |
| Not Applicable | Company | iSCSI SAN Storage | Bldg 4, Rm 7 | SAN Storage |
|  |  |  |  |  |
|  |  |  |  |  |

Table 10- 1. Hardware Components

**Note:** A complete and detailed list of the system hardware and softwareinventory is required per NIST SP 800-53, Rev 4 CM-8.

* 1. Software Inventory

The following table lists the principle software components for **<Information System Abbreviation>**.

*Instruction: Include any middleware, databases, or secure file transfer applications in this table. The first three rows are sample entries. The first three rows are sample entries. Add additional rows as needed.*

| Hostname | Function | Version | Patch Level | IP Address | Virtual (Yes / No) |
| --- | --- | --- | --- | --- | --- |
| hostname1.com | Physical Host for Virtual Infrastructure | XYZi.4.x vSphere | Update 1 | 255.255.255.254 | No |
| hostname2.com | Virtual Machine Application Server | Windows 2003 Server | SP2 | 255.255.255.253 | Yes |
| hostname3.com | Virtual Database SQL Server | 6.4.22 build 7 | SP1 | 255.255.255.252 | Yes |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 10- 2. Software Components

* 1. Network Inventory

The following table lists the principle network devices and components for **<Information System Abbreviation>**.

*Instruction: Include any switches, routers, hubs, and firewalls that play a role in protecting the information system, or that enable the network to function properly. The first three rows are sample entries. If all network devices and components are leveraged from a pre-existing Provisional Authorization, write “Leveraged” in the first column. Add additional rows as needed.*

| Hostname | Make | Model | IP Address | Function |
| --- | --- | --- | --- | --- |
| router-dallas | RouterCo | 2800 | 192.168.0.1 | router |
| switch-1 | SwitchCo | EZSX55W | 10.5.3.1 | switch |
| fw.company.com | FirewallCo | 21400, R71.x | 192.168.0.2 | firewall |
|  |  |  |  |  |

Table 10- 3. Network Components

* 1. Data Flow

*Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. See Guide to Understanding FedRAMP for a dataflow example. If necessary, include multiple data flow diagrams.*

<**insert diagram**>

Figure 10-2. Data Flow Diagram

* 1. Ports, Protocols and Services

The table below lists the Ports, Protocols, and Services enabled in this information system.

*Instruction: In the column labeled “Used By” indicate the components of the information system that make use of the ports, protocols, and services. In the column labeled “Purpose” indicate the purpose for the service (e.g. system logging, HTTP redirector, load balancing). This table must be consistent with CM-6 and CM-7. This table shall be completed, even if leveraging a pre-existing Provisional Authorization. Add more rows as needed.*

*Example is provided in row one of the table below and should be deleted.*

| Ports (TCP/UDP) | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
| 80/TCP | HTTP |  | Web | Tomcat |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 10- 4. Ports, Protocols, and Services

1. System Interconnections

*Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Indicate how the connection is being secured. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with CA-3.*

| CSP IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) | Data Direction (incoming, outgoing, or both) | Information Being Transmitted | Ports or Circuit # |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Table 11- 1. System Interconnections

1. Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the appropriate security control baseline standards are applied. Some of the control baselines have enhanced controls which are indicated in parenthesis.

Security controls that are representative of the sensitivity of <**Information System Abbreviation**> are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional FedRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parenthesis in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low and systems categorized as FIPS 199 Moderate use the controls designated as Moderate. A summary of which security standards pertain to which sensitivity level is found in the table that follows

| **ID** | **Control Description** | **Sensitivity Level** | |
| --- | --- | --- | --- |
| **Low** | **Moderate** |
| **Access Control (AC)** | |  |  |
| AC-1 | Access Control Policy and Procedures | AC-1 | AC-1 |
| AC-2 | Account Management | AC-2 | AC-2 (1, 2, 3, 4, 5, 7,  9, 10, 12) |
| AC-3 | Access Enforcement | AC-3 | AC-3 |
| AC-4 | Information Flow Enforcement | Not Selected | AC-4 (21) |
| AC-5 | Separation of Duties | Not Selected | AC-5 |
| AC-6 | Least Privilege | Not Selected | AC-6 (1, 2, 5, 9, 10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | AC-7 |
| AC-8 | System Use Notification | AC-8 | AC-8 |
| AC-10 | Concurrent Session Control | Not Selected | AC-10 |
| AC-11 | Session Lock | Not Selected | AC-11 (1) |
| AC-12 | Session Termination | Not Selected | AC-12 |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | AC-14 |
| AC-17 | Remote Access | AC-17 | AC-17 (1, 2, 3, 4, 9) |
| AC-18 | Wireless Access | AC-18 | AC-18 (1) |
| AC-19 | Access Control For Mobile Devices | AC-19 | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | AC-20(1, 2) |
| AC-21 | Information Sharing | Not Selected | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | AC-22 |
| **Awareness and Training (AT)** | |  |  |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | AT-1 |
| AT-2 | Security Awareness Training | AT-2 | AT-2 (2) |
| AT-3 | Role-Based Security Training | AT-3 | AT-3 |
| AT-4 | Security Training Records | AT-4 | AT-4 |
| **Audit and Accountability (AU)** | |  |  |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | AU-1 |
| AU-2 | Audit Events | AU-2 | AU-2 (3) |
| AU-3 | Content of Audit Records | AU-3 | AU-3 (1) |
| AU-4 | Audit Storage Capacity | AU-4 | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | AU-5 |
| AU-6 | Audit Review, Analysis, and Reporting | AU-6 | AU-6 (1, 3) |
| AU-7 | Audit Reduction and Report Generation | Not Selected | AU-7 (1) |
| AU-8 | Time Stamps | AU-8 | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | AU-9 (2, 4) |
| AU-11 | Audit Record Retention | AU-11 | AU-11 |
| AU-12 | Audit Generation | AU-12 | AU-12 |
| **Security Assessment and Authorization (CA)** | |  |  |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | CA-1 |
| CA-2 | Security Assessments | CA-2 (1) | CA-2 (1, 2, 3) |
| CA-3 | System Interconnections | CA-3 | CA-3 (3, 5) |
| CA-5 | Plan of Action and Milestones | CA-5 | CA-5 |
| CA-6 | Security Authorization | CA-6 | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 | CA-7 (1) |
| CA-8 | Penetration Testing | Not Selected | CA-8 (1) |
| CA-9 | Internal System Connections | CA-9 | CA-9 |
| **Configuration Management (CM)** | |  |  |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (1, 2, 3, 7) |
| CM-3 | Configuration Change Control | Not Selected | CM-3 |
| CM-4 | Security Impact Analysis | CM-4 | CM-4 |
| CM-5 | Access Restrictions For Change | Not Selected | CM-5 (1, 3, 5) |
| CM-6 | Configuration Settings | CM-6 | CM-6 (1) |
| CM-7 | Least Functionality | CM-7 | CM-7 (1, 2, 5) |
| CM-8 | Information System Component Inventory | CM-8 | CM-8 (1, 3, 5) |
| CM-9 | Configuration Management Plan | Not Selected | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 (1) |
| CM-11 | User-Installed Software | CM-11 | CM-11 |
| **Contingency Planning (CP)** | |  |  |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | CP-2 (1, 2, 3, 8) |
| CP-3 | Contingency Training | CP-3 | CP-3 |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 (1) |
| CP-6 | Alternate Storage Site | Not Selected | CP-6 (1, 3) |
| CP-7 | Alternate Processing Site | Not Selected | CP-7 (1, 2, 3) |
| CP-8 | Telecommunications Services | Not Selected | CP-8 (1, 2) |
| CP-9 | Information System Backup | CP-9 | CP-9 (1, 3) |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | CP-10 (2) |
| **Identification and Authentication (IA)** | |  |  |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1, 12) | IA-2 (1, 2, 3, 5, 8, 11, 12) |
| IA-3 | Device Identification and Authentication | Not Selected | IA-3 |
| IA-4 | Identifier Management | IA-4 | IA-4 (4) |
| IA-5 | Authenticator Management | IA-5 (1, 11) | IA-5 (1, 2, 3, 4, 6, 7, 11) |
| IA-6 | Authenticator Feedback | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1, 2, 3, 4) | IA-8 (1, 2, 3, 4) |
| **Incident Response (IR)** | |  |  |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | IR-2 |
| IR-3 | Incident Response Testing | Not Selected | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) |
| IR-5 | Incident Monitoring | IR-5 | IR-5 |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1, 2) |
| IR-8 | Incident Response Plan | IR-8 | IR-8 |
| IR-9 | Information Spillage Response | Not Selected | IR-9 (1, 2, 3, 4) |
| **Maintenance (MA)** | |  |  |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | MA-2 |
| MA-3 | Maintenance Tools | Not Selected | MA-3 (1, 2, 3) |
| MA-4 | Nonlocal Maintenance | MA-4 | MA-4 (2) |
| MA-5 | Maintenance Personnel | MA-5 | MA-5 (1) |
| MA-6 | Timely Maintenance | Not Selected | MA-6 |
| **Media Protection (MP)** | |  |  |
| MP-1 | Media Protection Policy and Procedures | MP-1 | MP-1 |
| MP-2 | Media Access | MP-2 | MP-2 |
| MP-3 | Media Marking | Not Selected | MP-3 |
| MP-4 | Media Storage | Not Selected | MP-4 |
| MP-5 | Media Transport | Not Selected | MP-5 (4) |
| MP-6 | Media Sanitization | MP-6 | MP-6 (2) |
| MP-7 | Media Use | MP-7 | MP-7 (1) |
| **Physical and Environmental Protection (PE)** | |  |  |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | PE-2 |
| PE-3 | Physical Access Control | PE-3 | PE-3 |
| PE-4 | Access Control For Transmission Medium | Not Selected | PE-4 |
| PE-5 | Access Control For Output Devices | Not Selected | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | PE-6 (1) |
| PE-8 | Visitor Access Records | PE-8 | PE-8 |
| PE-9 | Power Equipment and Cabling | Not Selected | PE-9 |
| PE-10 | Emergency Shutoff | Not Selected | PE-10 |
| PE-11 | Emergency Power | Not Selected | PE-11 |
| PE-12 | Emergency Lighting | PE-12 | PE-12 |
| PE-13 | Fire Protection | PE-13 | PE-13 (2, 3) |
| PE-14 | Temperature and Humidity Controls | PE-14 | PE-14 (2) |
| PE-15 | Water Damage Protection | PE-15 | PE-15 |
| PE-16 | Delivery and Removal | PE-16 | PE-16 |
| PE-17 | Alternate Work Site | Not Selected | PE-17 |
| **Planning (PL)** | |  |  |
| PL-1 | Security Planning Policy and Procedures | PL-1 | PL-1 |
| PL-2 | System Security Plan | PL-2 | PL-2 (3) |
| PL-4 | Rules of Behavior | PL-4 | PL-4 (1) |
| PL-8 | Information Security Architecture | Not Selected | PL-8 |
| **Personnel Security (PS)** | |  |  |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | PS-2 |
| PS-3 | Personnel Screening | PS-3 | PS-3 (3) |
| PS-4 | Personnel Termination | PS-4 | PS-4 |
| PS-5 | Personnel Transfer | PS-5 | PS-5 |
| PS-6 | Access Agreements | PS-6 | PS-6 |
| PS-7 | Third-Party Personnel Security | PS-7 | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | PS-8 |
| **Risk Assessment (RA)** | |  |  |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | RA-1 |
| RA-2 | Security Categorization | RA-2 | RA-2 |
| RA-3 | Risk Assessment | RA-3 | RA-3 |
| RA-5 | Vulnerability Scanning | RA-5 | RA-5 (1, 2, 3, 5, 6, 8) |
| **System and Services Acquisition (SA)** | |  |  |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | SA-4 (1, 2, 8, 9, 10) |
| SA-5 | Information System Documentation | SA-5 | SA-5 |
| SA-8 | Security Engineering Principles | Not Selected | SA-8 |
| SA-9 | External Information System Services | SA-9 | SA-9 (1, 2, 4, 5) |
| SA-10 | Developer Configuration Management | Not Selected | SA-10 (1) |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | SA-11 (1, 2, 8) |
| **System and Communications Protection (SC)** | |  |  |
| SC-1 | System and Communications Protection Policy and Procedures | SC-1 | SC-1 |
| SC-2 | Application Partitioning | Not Selected | SC-2 |
| SC-4 | Information In Shared Resources | Not Selected | SC-4 |
| SC-5 | Denial of Service Protection | SC-5 | SC-5 |
| SC-6 | Resource Availability | Not Selected | SC-6 |
| SC-7 | Boundary Protection | SC-7 | SC-7 (3, 4, 5, 7, 8, 12, 13, 18) |
| SC-8 | Transmission Confidentiality and Integrity | Not Selected | SC-8 (1) |
| SC-10 | Network Disconnect | Not Selected | SC-10 |
| SC-12 | Cryptographic Key Establishment and Management | SC-12 | SC-12 (2, 3) |
| SC-13 | Cryptographic Protection | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices | SC-15 | SC-15 |
| SC-17 | Public Key Infrastructure Certificates | Not Selected | SC-17 |
| SC-18 | Mobile Code | Not Selected | SC-18 |
| SC-19 | Voice Over Internet Protocol | Not Selected | SC-19 |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | SC-20 | SC-20 |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | SC-22 | SC-22 |
| SC-23 | Session Authenticity | Not Selected | SC-23 |
| SC-28 | Protection of Information At Rest | Not Selected | SC-28 (1) |
| SC-39 | Process Isolation | SC-39 | SC-39 |
| **System and Information Integrity (SI)** | |  |  |
| SI-1 | System and Information Integrity Policy and Procedures | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | SI-2 | SI-2 (2, 3) |
| SI-3 | Malicious Code Protection | SI-3 | SI-3 (1, 2, 7) |
| SI-4 | Information System Monitoring | SI-4 | SI-4 (1, 2, 4, 5, 14, 16, 23) |
| SI-5 | Security Alerts, Advisories, and Directives | SI-5 | SI-5 |
| SI-6 | Security Function Verification | Not Selected | SI-6 |
| SI-7 | Software, Firmware, and Information Integrity | Not Selected | SI-7 (1, 7) |
| SI-8 | Spam Protection | Not Selected | SI-8 (1, 2) |
| SI-10 | Information Input Validation | Not Selected | SI-10 |
| SI-11 | Error Handling | Not Selected | SI-11 |
| SI-12 | Information Handling and Retention | SI-12 | SI-12 |
| SI-16 | Memory Protection | Not Selected | SI-16 |

Table 13- 1. Summary of Required Security Controls

*Instruction: 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 the customer. Use the definitions in the table that follows to indicate where each security control originates from. Note that -1 Controls (AC-1, AU-1, SC-1 etc.) cannot be inherited and must be provided in some way by the service provider.*

*Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) 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.*

*In section 13, the NIST term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.*

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the CSP 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 system at the CSP and the control is not part of the standard corporate controls. | A unique host based intrusion detection system (HIDs) is available on the service offering 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 at the CSP. | There are scans of the corporate network infrastructure; scans of databases and web based application are system specific. |
| Configured by Customer | A control where the customer needs to apply a configuration in order 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 in order 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 the CSP and partially by the customer. | Security awareness training must be conducted by both the CSP and the customer. |
| Inherited from pre-existing Provisional Authorization | A control that is inherited from another CSP system that has already received a Provisional Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

Access Control (AC)

Access Control Policy and Procedures Requirements (AC-1)

The organization:

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

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

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

Account Management (AC-2)

The organization:

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

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(a): | |
| Parameter AC-2(e): | |
| Parameter AC-2(f): | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 |  |

Control Enhancement AC-2 (1)

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

| AC-2 (1) Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> |

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

Control Enhancement AC-2 (2)

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

| AC-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(2)-1: | |
| Parameter AC-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AC-2 (3)

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

**AC-2 (3) Parameter Requirement:** The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Authorizing Official.

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter AC-2(3): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid(Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (4)

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

| AC-2 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (4) What is the solutions and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (5)

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

| AC-2 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (5) What is the solutions and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (7)

The organization:

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

| AC-2 (7) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(7)(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AC-2 (9)

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

**AC-2 (9) Additional FedRAMP Requirements and Guidance:** Required if shared/group accounts are deployed.

| AC-2 (9) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(9): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (10)

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

**AC-2 (10) Additional FedRAMP Requirements and Guidance:** Required if shared/group accounts are deployed.

| AC-2 (10) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (12)

The organization:

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

**AC-2 (12)(a) and AC-2 (12)(b) Additional FedRAMP Requirements and Guidance:** Required for privileged accounts.

| AC-2 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(12)(a) | |
| Parameter AC-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Access Enforcement (AC-3)

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

| AC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Information Flow Enforcement (AC-4)

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

| AC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-4 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-4 (21)

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

| AC-4 (21) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-4(21)-1: | |
| Parameter AC-4(21)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
|  |

Separation of Duties (AC-5)

The organization:

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

**AC-5 Additional FedRAMP Requirements and Guidance:** Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP.

| AC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Least Privilege (AC-6)

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

| AC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-6 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-6 (1)

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

| AC-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-6 (2)

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

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

| AC-6 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-6 (5)

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

| AC-6 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-6 (9)

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-6 (10)

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

| AC-6 (10) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
|  |

Unsuccessful Login Attempts (AC-7)

The organization:

1. Enforces a limit of [*FedRAMP Assignment: not more than three*] consecutive invalid logon attempts by a user during a [*FedRAMP Assignment: fifteen minutes*]; and
2. Automatically [*Selection: locks the account/node for an* [*FedRAMP Assignment: thirty minutes*]; *locks the account/node until released by an administrator; delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

**AC-7 Additional FedRAMP Requirements and Guidance:** Guidance: FedRAMP considers remote admin access by VPN to be remote access.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-7(a)-1: | |
| Parameter AC-7(a)-2: | |
| Parameter AC-7(b)-1: | |
| Parameter AC-7(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

System Use Notification (AC-8)

The information system:

1. Displays to users [*Assignment: organization-defined system use notification message or banner (See Additional Requirements and Guidance)*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [*Assignment: organization-defined conditions (See Additional Requirements and Guidance)*], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

**AC-8 Additional FedRAMP Requirements and Guidance:**

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

**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.

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

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

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

**Additional FedRAMP Requirements and Guidance**

**Requirement 1:** 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.

**Requirement 2:** 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. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

**Requirement 3:** 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.

| AC-8 | Additional FedRAMP 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |
| Req. 2 |  |
| Req. 3 |  |

Concurrent Session Control (AC-10)

The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access*].

| AC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-10 What is the solution and how is it implemented? |
| --- |
|  |

Session Lock (AC-11)

The information system:

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

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-11(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 (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AC-11 (1)

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

| AC-11 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
|  |

Session Termination (AC-12)

The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

| AC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-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 (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-11 What is the solution and how is it implemented? |
| --- |
|  |

Permitted Actions without Identification or Authentication (AC-14)

The organization:

1. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Remote Access (AC-17)

The organization:

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

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AC-17 (1)

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-17 (2)

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

| AC-17 (2) | Control Enhancement 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  Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-17 (3)

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

| AC-17 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-17(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  Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-17 (4)

The organization

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

|  |  |
| --- | --- |
| AC-17 (4) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter AC-17(4)(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  Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AC-17 (9)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [*FedRAMP Assignment: no greater than fifteen minutes*].

| AC-17 (9) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-17(9): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
|  |

Wireles Access Restrictions (AC-18)

The organization:

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

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AC-18 (1)

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

| AC-18 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-18(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
|  |

Access Control for Portable and Mobile Systems (AC-19)

The organization:

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

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AC-19 (5)

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

| AC-19 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-19(5)-1: | |
| Parameter AC-19(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 (Corporate and System Specific)  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-19 (5) What is the solution and how is it implemented? |
| --- |
|  |

Use of External Information Systems (AC-20)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

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

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AC-20 (1)

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

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

| AC-20 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AC-20 (2)

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

| AC-20 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-20(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
|  |

Publicly Accessible Content (AC-21)

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and
2. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

| AC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-21(a): | |
| Parameter AC-21(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Publicly Accessible Content (AC-22)

The organization:

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

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-22(d): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Awareness and Training (AT)

Security Awareness and Training Policy and Procedures (AT-1)

The organization:

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

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

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

Security Awareness (AT-2)

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

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

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-2(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AT-2 (2)

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

| AT-2 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Role-Based Security Training (AT-3)

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

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

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AT-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Security Training Records (AT-4)

The organization:

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

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Audit and Accountability (AU)

Audit and Accountability Policy and Procedures (AU-1)

The organization:

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

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

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

Audit Events (AU-2)

The organization:

1. Determines that the information system is capable of auditing the following events: [*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*];
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [*FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event*].

| AU-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-2(a): | |
| Parameter AU-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement AU-2 (3)

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

**AU-2 (3) Additional FedRAMP Requirements and Guidance:** Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB.

| AU-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

Content of Audit Records (AU-3)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

| AU-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-3 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AU-3 (1)

The information system generates audit records containing the following additional information: [*FedRAMP Assignment:* [*session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon*]].

**AU-3 (1) Additional FedRAMP Requirements and Guidance:** **Requirement:** The service provider defines audit record types. The audit record types are approved and accepted by the JAB.

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

| AU-3 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-3(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
|  |

Audit Storage Capacity (AU-4)

The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Response to Audit Processing Failures (AU-5)

The information system:

1. Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and
2. Takes the following additional actions: [*FedRAMP Assignment: low-impact: overwrite oldest audit records; moderate-impact: shut down*].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-5(a): | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Audit Review, Analysis, and Reporting (AU-6)

The organization:

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

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AU-6 (1)

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

| AU-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AU-6 (3)

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

| AU-6 (3) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
|  |

Audit Reduction and Report Generation (AU-7)

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

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

| AU-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Corporate (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AU-7 (1)

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

| AU-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-7(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-7 (1) What is the solution and how is it implemented? |
| --- |
|  |

Time Stamps (AU-8)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*].

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement AU-8 (1)

The information system:

1. Compares the internal information system clocks [*FedRAMP Assignment: at least hourly*] with [*FedRAMP Assignment: authoritative time source:* [*http://tf.nist.gov/tf-cgi/servers.cgi*](http://tf.nist.gov/tf-cgi/servers.cgi)]; and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

| AU-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-8(1)(a)-1: | |
| Parameter AU-8(1)(a)-2:: | |
| Parameter AU-8(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-8(1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

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

**Requirement 1:** The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

**Requirement 2:** The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

**Guidance:** Synchronization of system clocks improves the accuracy of log analysis.

| AU-8 (1) | Additional Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |
| Req. 2 |  |

Protection of Audit Information (AU-9)

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

| AU-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-9 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AU-9 (2)

The information system backs up audit records [*FedRAMP Assignment: at least weekly*] onto a physically different system or system component than the system or component being audited.

| AU-9 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AU-9 (4)

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

| AU-9 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AU-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
|  |

Audit Record Retention (AU-11)

The organization retains audit records for [*FedRAMP Assignment: at least ninety days*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

**AU-11 Additional FedRAMP Requirements and Guidance:** Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-11 What is the solution and how is it implemented? |
| --- |
|  |

Audit Generation (AU-12)

The information system:

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

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Security Assessment and Authorization (CA)

Certification, Authorization, Security Assessment Policies and Procedures (CA-1)

The organization:

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

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

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Security Assessments (CA-2)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [*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 requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [*FedRAMP Assignment: individuals or roles to include the FedRAMP PMO*].

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-2(b): | |
| Parameter CA-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CA-2 (1)

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to conduct security control assessments.

**CA-2 (1) Additional FedRAMP Requirements and Guidance:** Requirement: Must use an accredited 3PAO for JAB authorization.

| CA-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-2(1): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CA-2 (2)

The organization includes as part of security control assessments, [*FedRAMP Assignment: at least annually*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing;* [*Assignment: organization-defined other forms of security assessment*]].

**CA-2 (2) Additional FedRAMP Requirements and Guidance:** Requirement: To include 'announced', 'vulnerability scanning to occur at least annually.'

| CA-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-2(2)-1: | |
| Parameter CA-2(2)-2: | |
| Parameter CA-2(2)-3: | |
| Parameter CA-2(2)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CA-2 (3)

The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*FedRAMP Assignment: any 3PAO*] when the assessment meets [*FedRAMP Assignment: the conditions of a P-ATO in the FedRAMP Secure Repository*].

| CA-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-2(3)-1: | |
| Parameter CA-2(3)-2: | |
| Parameter CA-2(3)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

System Interconnections (CA-3)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [*FedRAMP Assignment: 3 years / annually and on input from FedRAMP*].

| System Name | Name of Organization CSP System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 13- 2. Authorized Connections

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | See § 11 for information about implementation. |
| Part b | See Table 13-2 and Table 11-1 in § 11 for information about implementation. |
| Part c |  |

Control Enhancement CA-3 (3)

The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*FedRAMP Assignment; Boundary Protections which meet Trusted Internet Connection (TIC) requirements*].

**CA-3 (3) Additional FedRAMP Requirements and Guidance:** Refer to Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document.

| CA-3 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-3(3)-1: | |
| Parameter CA-3(3)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CA-3 (5)

The organization employs [*Selection: allow-all, deny-by-exception; deny-all, permit-by-exception*] policy for allowing [*Assignment: organization-defined information systems]* to connect to external information systems.]

**CA-3 (5) Additional FedRAMP Requirements and Guidance: Guidance:** For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing

| CA-3 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-3(5)-1: | |
| Parameter CA-3(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
|  |

Plan of Action and Milestones (CA-5)

The organization:

1. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones [*FedRAMP Assignment: at least monthly*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

**CA-5 Additional FedRAMP Requirements and Guidance:** **Requirement:** POA&Ms must be provided at least monthly.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Security Authorization (CA-6)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [*FedRAMP Assignment: at least every three years or when a significant change occurs*].

**CA-6c Additional FedRAMP Requirements and Guidance:** Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. 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 Authorizing Official.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Continuous Monitoring (CA-7)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [*Assignment: organization-defined metrics*] to be monitored;
2. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [*FedRAMP Assignment: to meet Federal and FedRAMP requirements*] [*Assignment: organization-defined frequency*].

**CA-7 Additional FedRAMP Requirements and Guidance:** CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 Additional FedRAMP Requirements and Guidance:**

**Requirement 1:** Operating System Scans: at least monthly

**Requirement 2:** Database and Web Application Scans: at least monthly

**Requirement 3:** All scans performed by Independent Assessor: at least annually

| CA-7 | Additional Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |
| Req. 2 |  |
| Req. 3 |  |

Control Enhancement CA-7 (1)

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to monitor the security controls in the information system on an ongoing basis.

| CA-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-7(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
|  |

Penetration Testing (CA-8)

The organization conducts penetration testing [*FedRAMP Assignment: at least annually*] on [*Assignment: organization-defined information systems or system components*].

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CA-8 (1)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| CA-8 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Internal System CONNECTIONS (CA-9)

The organization:

1. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CA-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Configuration Management (CM)

Configuration Management Policies and Procedures (CM-1)

The organization:

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

| CM-1 | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-1(a): | |
| Parameter CM-1(b)(1): | |
| Parameter CM-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Baseline Configuration (CM-2)

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

| CM-2 | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-2 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CM-2 (1)

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

1. [*FedRAMP Assignment: Annually*];
2. When required due to [*FedRAMP Assignment: when directed by the JAB*]; and
3. As an integral part of information system component installations and upgrades.

| CM-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-2(1)(a): | |
| Parameter CM-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement CM-2 (2)

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

| CM-2 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CM-2 (3)

The organization retains [*Assignment*: *organization-defined previous versions of baseline configurations of the information system*] to support rollback.

| CM-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CM-2 (7)

The organization:

1. Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

| CM-2 (7) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-2(7)(a)-1: | |
| Parameter CM-2(7)(a)-2: | |
| Parameter CM-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Configuration Change Control (CM-3)

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];
6. Audits and reviews activities associated with configuration-controlled changes to the information system; and
7. Coordinates and provides oversight for configuration change control activities through [*FedRAMP Assignment: See additional FedRAMP requirements and guidance*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

**CM-3e Additional FedRAMP Requirements and Guidance: Guidance:** In accordance with record retention policies and procedures.

**CM-3g Additional FedRAMP Requirements and Guidance:**

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

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-3(e): | |
| Parameter CM-3(g)-1 | |
| Parameter CM-3(g)-2 | |
| Parameter CM-3(g)-3 | |
| Parameter CM-3(g)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

Security Impact Analysis (CM-4)

The organization analyzes changes to the information system to determine potential security 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Access Restrictions for Change (CM-5)

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

| CM-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CM-5 (1)

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

| CM-5 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CM-5 (3)

The information system prevents the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

**CM-5(3) Additional FedRAMP Requirements and Guidance:** If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| CM-5 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CM-5 (5)

The organization:

1. Limits privileges to change information system components and system-related information within a production or operational environment; and
2. Reviews and reevaluates privileges [*FedRAMP Assignment: at least quarterly*].

| CM-5 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Configuration Settings (CM-6)

The organization:

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

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

**Requirement 1:** The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available.

**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).

**Guidance:** Information on the USGCB checklists can be found at: <http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc>.

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

**Note:** Information on the USGCB checklists can be found at: [*http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc\*](http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc\)

Information on SCAP can be found at:[*http://scap.nist.gov/*](http://scap.nist.gov/)

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CM-6 (1)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

| CM-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
|  |

Least Functionality (CM-7)

The organization:

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

**CM-7 Additional FedRAMP Requirements and Guidance:** **Requirement:** The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available.

**Guidance:** Information on the USGCB checklists can be found at: <http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc>.

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

|  |  |
| --- | --- |
| CM-7 What is the solution and how is it implemented? | |
| Part a |  |
| Part b |  |

Control Enhancement CM-7 (1)

The organization:

1. Reviews the information system [*FedRAMP Assignment: at least Monthly*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].

| CM-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-7(1)(a): | |
| Parameter CM-7(1)(b): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement CM-7 (2)

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

**CM-7(2) Additional FedRAMP Requirements and Guidance:** Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e. white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

| CM-7 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-7(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CM-7 (5)

The organization:

1. Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [*FedRAMP Assignment: at least annually or when there is a change.*].

| CM-7 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-7(5)(a): | |
| Parameter CM-7(5)(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Information System Component Inventory (CM-8)

The organization:

1. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and
2. Reviews and updates the information system component inventory [*FedRAMP Assignment: at least monthly*].

**CM-8 Additional FedRAMP Requirements and Guidance:** **Requirement:** Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-8(a)(4): | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement CM-8 (1)

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

*Instruction: A description of the inventory information is documented in Section 10. It is not necessary to re-document it here.*

| CM-8 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CM-8 (3)

The organization:

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

| CM-8 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-8(3)(a): | |
| Parameter CM-8(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement CM-8 (5)

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

| CM-8 (5) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
|  |

Configuration Management Plan (CM-9)

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

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

| CM-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Software Usage Restrictions (CM-10)

The organization:

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

| CM-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement CM-10 (1)

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

| CM-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CM-10(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-10 What is the solution and how is it implemented? |
| --- |
|  |

Configuration Management Plan (CM-11)

The organization:

1. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;
2. Enforces software installation policies through [*Assignment: organization-defined methods*]; and
3. Monitors policy compliance at [*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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Contingency Planning (CP)

Contingency Planning Policy and Procedures (CP-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy [*FedRAMP Assignment: at least every three years*].; and
   2. Contingency planning procedures [*FedRAMP Assignment: at least annually*].

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

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Contingency Plan (CP-2)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions 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 missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
2. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [*FedRAMP Assignment: at least annually*];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

**CP-2 Additional FedRAMP Parameter Requirement:** For JAB authorizations the contigency lists include designated FedRAMP personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-2(a).(6) | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 |  |

Control Enhancement CP-2 (1)

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

| CP-2 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CP-2 (2)

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

| CP-2 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CP-2 (3)

The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

| CP-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-2 (8)

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

| CP-2 (8) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
|  |

Contingency Training (CP-3)

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

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

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-3(a): | |
| Parameter CP-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-3 What is the solution and how is it implemented? |
| --- |
|  |

Contingency Plan Testing (CP-4)

The organization:

1. Tests the contingency plan for the information system [*FedRAMP Assignment: at least annually for moderate impact systems; at least every three years for low impact systems*] using [*FedRAMP Assignment: functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

**CP-4(a) Additional FedRAMP Requirements and Guidance:** Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the Authorizing Official prior to initiating testing.

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

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement CP-4 (1)

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

| CP-4 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
|  |

Alternate Storage Site (CP-6)

The organization:

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

| CP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement CP-6 (1)

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

| CP-6 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-6 (3)

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions**.**

| CP-6 (3) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
|  |

Alternate Processing Site (CP-7)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*FedRAMP Assignment: See additional FedRAMP requirements and guidance*] when the primary processing capabilities are unavailable;

**CP-7a Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-7(a)-1: | |
| Parameter CP-7(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement CP-7 (1)

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

**CP-7(1) Additional FedRAMP Requirements and Guidance:**  The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites will be less relevant.

| CP-7 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-7 (2)

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-7 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-7 (3)

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

| CP-7 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
|  |

Telecommunications Services (CP-8)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*FedRAMP Assignment: See CP-8 additional FedRAMP requirements and guidance*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**CP-8 Additional FedRAMP Requirements and Guidance:** Requirement: The service provider defines a time period consistent with the business impact analysis.

| CP-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-8-1: | |
| Parameter CP-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  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-8 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-8 (1)

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

| CP-8 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement CP-8 (2)

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

| CP-8 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
|  |

Information System Backup (CP-9)

The organization:

1. Conducts backups of user-level information contained in the information system [*FedRAMP Assignment: daily incremental; weekly full*]

**CP-9(a) Additional FedRAMP Requirements and Guidance:** Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.

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

**CP-9(b)** **Additional FedRAMP Requirements and Guidance:** Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.

1. Conducts backups of information system documentation including security-related documentation [*FedRAMP Assignment: daily incremental; weekly full* ]; and

**CP-9(c)** **Additional FedRAMP Requirements and Guidance:** Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB

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

**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.

Requirement: The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-9(a): | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Control Enhancement CP-9 (1)

The organization tests backup information [*FedRAMP Assignment: at least annually*] to verify media reliability and information integrity.

| CP-9 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-9 (3)

The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

| CP-9 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter CP-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
|  |

Information System Recovery and Reconstitution (CP-10)

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

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-10 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement CP-10 (2)

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

| CP-10 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
|  |

Identification and Authentication (IA)

Identification and Authentication Policy and Procedures (IA-1)

The organization:

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

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

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

User Identification and Authentication (IA-2)

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

|  |  |
| --- | --- |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-2 (1)

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

| IA-2 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-2 (2)

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

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-2 (3)

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

| IA-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-2 (5)

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

| IA-2 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-2 (8)

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

| IA-2 (8) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-2 (8) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-2 (11)

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

| IA-2 (11) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-2(11): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-2 (11) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-2 (12)

| IA-2 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

**IA-2 (12) Additional FedRAMP Requirements and Guidance:** Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
|  |

Device Identification and Authentication (IA-3)

The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

| IA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-3-1: | |
| Parameter IA-3-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-3 What is the solution and how is it implemented? |
| --- |
|  |

Identifier Management (IA-4)

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

1. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [*Assignment: at least two years*]; and
5. Disabling the identifier after [*Assignment: ninety days for user identifiers; see additional requirements and guidance*]

**IA-4e Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines time period of inactivity for device identifiers.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-4(a): | |
| Parameter IA-4(d): | |
| Parameter IA-4(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-4 (4)

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

| IA-4 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-4(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Authenticator Management (IA-5)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [*FedRAMP* *Assignment: to include 60 days for passwords*].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(g): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 |  |
| Part j |  |

Control Enhancement IA-5 (1)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [*FedRAMP* *Assignment:* [*case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters*];
2. Enforces at least the following number of changed characters when new passwords are created: [*FedRAMP* *Assignment: at least one*];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [*FedRAMP* *Assignment: one day minimum, sixty day maximum*];
5. Prohibits password reuse for [*FedRAMP* *Assignment: twenty-four*] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

| IA-5 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(1)(a): | |
| Parameter IA-5(1)(b): | |
| Parameter IA-5(1)(d): | |
| Parameter IA-5(1)(e): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

Control Enhancement IA-5 (2)

The information system, for PKI-based authentication:

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

| IA-5 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Control Enhancement IA-5 (3)

The organization requires that the registration process to receive [*FedRAMP* *Assignment: All hardware/biometric (multifactor authenticators*] be conducted [*FedRAMP* *Selection: in person*] before [*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].

| IA-5 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(3)-1: | |
| Parameter IA-5(3)-2: | |
| Parameter IA-5(3)-3: | |
| Parameter IA-5(3)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-5 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-5 (4)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

**IA-5(4) Additional FedRAMP Requirements and Guidance:** Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators

| IA-5 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-5 (4) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-5 (6)

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

| IA-5 (6) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-5 (6) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-5 (7)

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

| IA-5 (7) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-5 (7) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-5 (11)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].

| IA-5 (11) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Authenticator Feedback (IA-6)

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

| IA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Cryptographic Module Authentication (IA-7)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

| IA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Identification and Authentication (Non-Organizational Users) (IA-8)

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

| IA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-8 (1)

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

| IA-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IA-8 (2)

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

| IA-8 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-8 (3)

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.

| IA-8 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IA-8(3): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IA-8 (4)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Incident Response (IR)

Incident Response Policy and Procedures (IR-1)

The organization:

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

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

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

Incident Response Training (IR-2)

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

1. Within to [*Assignment: organization-defined personnel or roles*]of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [*FedRAMP Assignment: at least annually*] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IR-2(a):: | |
| Parameter IR-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Incident Response Testing (IR-3)

The organization tests the incident response capability for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: See Additional FedRAMP Requirements and Guidance*] to determine the incident response effectiveness and documents the results.

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

|  |  |
| --- | --- |
| IR-3 | Control Summary Information |
| Responsible Role: | |
| Parameter IR-3-1: | |
| Parameter IR-3-2: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA>** | |

| IR-3 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IR-3 (2)

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

|  |  |
| --- | --- |
| IR-3 (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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | | |

|  |
| --- |
| IR-3 (2) What is the solution and how is it implemented? |
|  |

Incident Handling (IR-4)

The organization:

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

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

| IR-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement IR-4 (1)

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

| IR-4 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
|  |

Incident Monitoring (IR-5)

The organization tracks and documents information system security incidents.

| IR-5 | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Incident Reporting (IR-6)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [*FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)*]; and
2. Reports security incident information to [*Assignment: organization-defined authorities*].

**IR-6 Additional FedRAMP Requirements and Guidance: Requirement:** Report security incident information according to FedRAMP Incident Communications Procedure

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement IR-6 (1)

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

| IR-6 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-6 (1) What is the solution and how is it implemented? |
| --- |
|  |

Incident Response Assistance (IR-7)

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

| IR-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement IR-7 (1)

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

| IR-7 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-7 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement IR-7 (2)

The organization:

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

| IR-7 (2) | Control Enhancement 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  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Incident Response Plan (IR-8)

The organization:

1. Develops an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization.
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
2. Distributes copies of the incident response plan to [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*]

**IR-8(b) Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Reviews the incident response plan [*FedRAMP Assignment: at least annually*];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [*FedRAMP Assignment: See Additional FedRAMP Requirements and Guidance*]

**IR-8(e) Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

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

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter IR-8(a)(8): | |
| Parameter IR-8(b): | |
| Parameter IR-8(c): | |
| Parameter IR-8(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

Information Spillage Response (IR-9)

The organization responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [*Assignment: organization-defined actions*].

|  |  |
| --- | --- |
| IR-9 | Control Summary Information |
| Responsible Role: | |
| Parameter IR-9(b): | |
| Parameter IR-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | | |

|  |  |
| --- | --- |
| IR-9 What is the solution and how is it implemented? | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

Control Enhancement IR-9 (1)

The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

|  |  |
| --- | --- |
| IR-9 (1) | Control Summary Information |
| Responsible Role: | |
| Parameter IR-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | | |

|  |
| --- |
| IR-9 (1) What is the solution and how is it implemented? |
|  |

Control Enhancement IR-9 (2)

The organization provides information spillage response training [*Assignment: organization defined frequency*].

|  |  |
| --- | --- |
| IR-9 (2) | Control Summary Information |
| Responsible Role: | |
| Parameter IR-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | | |

|  |
| --- |
| IR-9 (2) What is the solution and how is it implemented? |
|  |

Control Enhancement IR-9 (3)

The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

|  |  |
| --- | --- |
| IR-9 (3) | Control Summary Information |
| Responsible Role: | |
| Parameter IR-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | | |

|  |
| --- |
| IR-9 (3) What is the solution and how is it implemented? |
|  |

Control Enhancement IR-9 (4)

The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

|  |  |
| --- | --- |
| IR-9 (4) | Control Summary Information |
| Responsible Role: | |
| Parameter IR-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | | |

|  |
| --- |
| IR-9 (4) What is the solution and how is it implemented? |
|  |

Maintenance (MA)

System Maintenance Policy and Procedures (MA-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy [*FedRAMP Assignment: at least every three years*]; and
   2. System maintenance procedures [*FedRAMP Assignment: at least annually*].

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

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

Controlled Maintenance (MA-2)

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes *[Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

| MA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MA-2(c): | |
| 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) | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |

Maintenance Tools (MA-3)

The organization approves, controls, and monitors information system maintenance tools.

| MA-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-3 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement MA-3 (1)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| MA-3 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-3 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement MA-3 (2)

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

| MA-3 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-3 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement MA-3 (3)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

1. Verifying that there is no organizational information contained on the equipment;
2. Sanitizing or destroying the equipment;
3. Retaining the equipment within the facility; or
4. Obtaining an exemption from [*FedRAMP Assignment: the information owner*]explicitly authorizing removal of the equipment from the facility.

| MA-3 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MA-3(3)(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Remote Maintenance (MA-4)

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement MA-4 (2)

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

| MA-4 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-4 (2) What is the solution and how is it implemented? |
| --- |
|  |

Maintenance Personnel (MA-5)

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement MA-5 (1)

The organization:

1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system

**MA-5 (1) Additional FedRAMP Requirements and Guidance:** Requirement: Only MA-5 (1)(a)(1) is required by FedRAMP Moderate Baseline

| MA-5 (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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Timely Maintenance (MA-6)

The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*]of failure.

| MA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MA-6-1: | |
| Parameter MA-6-2: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MA-6 What is the solution and how is it implemented? |
| --- |
|  |

Media Protection (MP)

Media Protection Policy and Procedures (MP-1)

The organization:

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

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

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Media Access (MP-2)

The organization restricts 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Media Labeling (MP-3)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [*FedRAMP Assignment: no removable media types*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas* *FedRAMP Assignment: parameter not applicable*]

**MP-3(b) Additional FedRAMP Requirements and Guidance:** **Guidance:** Second parameter in MP-3(b) is not applicable.

| MP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-3(b)-1: | |
| Parameter MP-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Media Storage (MP-4)

The organization:

1. Physically controls and securely stores [*FedRAMP Assignment: [all types of digital and non-digital media with sensitive information*] within [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*]; and

**MP-4a Additional FedRAMP Requirements and Guidance:** **Requirement:** The service provider defines controlled areas within facilities where the information and information system reside.

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

| MP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-4(a)-1: | |
| Parameter MP-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Media Transport (MP-5)

The organization:

1. Protects and controls [*FedRAMP Assignment: all media with sensitive information*] during transport outside of controlled areas using [*FedRAMP Assignment:* *for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container*];

**MP-5a Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.

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

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-5(a)-1: | |
| Parameter MP-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MP-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Control Enhancement MP-5 (4)

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

| MP-5 (4) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
|  |

Media Sanitization and Disposal (MP-6)

The organization:

1. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with strength and integrity commensurate with the classification 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement MP-6 (2)

The organization tests sanitization equipment and procedures [*FedRAMP Assignment: at least annually*] to verify that the intended sanitization is being achieved.

**MP-6(2) Additional FedRAMP Requirements and Guidance: Guidance:** Equipment and procedures may be tested or evaluated for effectiveness.

| MP-6 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter MP-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
|  |

Media Use (MP-7)

The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

|  |  |
| --- | --- |
| MP-7 | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter MP-7-1: | |
| Parameter MP-7-2: | |
| Parameter MP-7-3: | |
| Parameter MP-7-4: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | |

|  |
| --- |
| MP-7 What is the solution and how is it implemented? |
|  |

Control Enhancement MP-7 (1)

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

|  |  |
| --- | --- |
| MP-7 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

|  |
| --- |
| MP-7 (1) What is the solution and how is it implemented? |
|  |

Physical and Environmental Protection (PE)

Physical and Environmental Protection Policy and Procedures (PE-1)

The organization:

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

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-1(a): | |
| Parameter PE-1(b)(1): | |
| Parameter PE-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Physical Access Authorizations (PE-2)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [*FedRAMP Assignment: at least annually*]; and
4. Removes 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Physical Access Control (PE-3)

The organization:

1. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [*FedRAMP Assignment: CSP defined physical access control systems/devices and guards*];
2. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];
3. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [*FedRAMP Assignment: in all circumstances within restricted access area where the information system resides*];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [*Assignment: organization-defined physical access devices*] every [*FedRAMP Assignment: at least annually*]; and
7. Changes combinations and keys [*FedRAMP Assignment: at least annually*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Enhancement 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): | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 |  |

Access Control for Transmission Medium (PE-4)

The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

| PE-4 | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-4-1 | |
| Parameter PE-4-2 | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-4 What is the solution and how is it implemented? |
| --- |
|  |

Access Control for Output Devices (PE-5)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| PE-5 | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-5 What is the solution and how is it implemented? |
| --- |
|  |

Monitoring Physical Access (PE-6)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [*FedRAMP Assignment: at least monthly*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and
3. Coordinates results of reviews and investigations with the organization’s 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement PE-6 (1)

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | Control Enhancement 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)  Hybrid (Service Provider and Customer)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-6 (1) What is the solution and how is it implemented? |
| --- |
|  |

Visitor Access Records (PE-8)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [*FedRAMP Assignment: for a minimum of one year*]; and
2. Reviews visitor access records [*FedRAMP Assignment: at least monthly*]

| PE-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-8(a): | |
| Parameter PE-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Power Equipment and Cabling (PE-9)

The organization protects power equipment and power cabling for the information system from damage and destruction.

| PE-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-9 What is the solution and how is it implemented? |
| --- |
|  |

Emergency Shutoff (PE-10)

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| PE-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-10(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Emergency Power (PE-11)

The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

| PE-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-11 What is the solution and how is it implemented? |
| --- |
|  |

Emergency Lighting (PE-12)

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Fire Protection (PE-13)

The organization employs and maintains fire suppression and detection devices/systems for the information system 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement PE-13 (2)

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*].

| PE-13 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-13(2)-1: | |
| Parameter PE-13(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-13 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement PE-13 (3)

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| PE-13 (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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-13 (3) What is the solution and how is it implemented? |
| --- |
|  |

Temperature and Humidity Controls (PE-14)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [*FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments*]; and
2. Monitors temperature and humidity levels [*FedRAMP Assignment: continuously*]

**PE-14(a) Additional FedRAMP Requirements and Guidance: 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): | |
| Parameter PE-14(b) | |
| Parameter PE-14(b) Additional: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement PE-14 (2)

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

|  |  |
| --- | --- |
| PE-14 (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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Water Damage Protection (PE-15)

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

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Delivery and Removal (PE-16)

The organization authorizes, monitors, and controls [*FedRAMP Assignment: all information system components*] entering and exiting the facility and maintains records of those items.

| PE-16 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-16: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-16 What is the solution and how is it implemented? |
| --- |
|  |

Alternate Work Site (PE-17)

The organization:

1. Employs [*Assignment: organization-defined security controls*] at alternate work sites*;*
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| PE-17 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PE-17(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)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PE-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Planning (PL)

Security Planning Policy and Procedures (PL-1)

The organization:

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

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PL-1(a): | |
| Parameter PL-1(b)(1): | |
| Parameter PL-1(b)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

System Security Plan (PL-2)

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information ;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];
3. Reviews the security plan for the information system [*FedRAMP Assignment: at least annually*];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Control Enhancement PL-2 (3)

The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.

|  |  |
| --- | --- |
| PL-2 (3) | Control Summary Information |
| Responsible Role: | |
| Parameter PL-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

.

|  |
| --- |
| PL-2 (3) What is the solution and how is it implemented? |
|  |

Rules of Behavior (PL-4)

The organization:

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

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PL-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Control Enhancement PL-4 (1)

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

|  |  |
| --- | --- |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | |

|  |
| --- |
| PL-4 (1) What is the solution and how is it implemented? |
|  |

Information Security Architecture (PL-8)

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. Reviews and updates the information security architecture [*FedRAMP Assignment: at least annually*] to reflect updates in the enterprise architecture; and
3. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions

| PL-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PL-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Personnel Security (PS)

Personnel Security Policy and Procedures (PS-1)

The organization:

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

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

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

Position Categorization (PS-2)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Personnel Screening (PS-3)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [*FedRAMP* *Assignment: for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement PS-3 (3)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

1. Have valid access authorizations that are demonstrated by assigned official government duties; and
2. Satisfy [*FedRAMP Assignment: personnel screening criteria – as required by specific information*].

|  |  |
| --- | --- |
| PS-3 (3) | Control Summary Information |
| Responsible Role: | |
| Parameter PS-3 (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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | | |

|  |
| --- |
| PS-3 (3) What is the solution and how is it implemented? |
|  |

Personnel Termination (PS-4)

The organization, upon termination of individual employment:

1. Disables information system access within [*FedRAMP Assignment: same day*];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter PS-4(a) | |
| Parameter PS-4(c) | |
| Parameter PS-4(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Personnel Transfer (PS-5)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [*Assignment: organization-defined personnel or roles*] within [*FedRAMP Assignment: within five days of the formal transfer action (DoD 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Access Agreements (PS-6)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [*FedRAMP Assignment: at least annually*]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*FedRAMP Assignment: at least annually*].

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Third-Party Personnel Security (PS-7)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*FedRAMP Assignment: same day*]; and
5. Monitors provider compliance.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Personnel Sanctions (PS-8)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Risk Assessment (RA)

Risk Assessment Policy and Procedures (RA-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [*FedRAMP Assignment: at least every three years*]; and
   2. Risk assessment procedures [*FedRAMP Assignment: at least annually*].

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

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

Security Categorization (RA-2)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the Authorizing Official or authorizing official designated representative.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Risk Assessment (RA-3)

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*FedRAMP Assignment: security assessment report*]];
3. Reviews risk assessment results [*FedRAMP Assignment: at least every three years or when a significant change occurs*];
4. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and
5. Updates the risk assessment [*FedRAMP Assignment: at least every three years or when a significant change occurs*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

**RA-3 Additional FedRAMP Requirements and Guidance:** **Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

**RA-3d Additional FedRAMP Requirements and Guidance:** **Requirement:** Requirement to include the Authorizing Official; for JAB authorizations to include FedRAMP.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter RA-3(b): | |
| Parameter RA-3(c): | |
| Parameter RA-3(d): | |
| Parameter RA-3(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Vulnerability Scanning (RA-5)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications

[*FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

**RA-5(a) Additional FedRAMP Requirements and Guidance:** **Requirement:** An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [*FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate risk vulnerabilities mitigated within ninety days from date of discovery*], in accordance with an organizational assessment of risk; and
4. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**RA-5(e) Additional FedRAMP Requirements and Guidance:** Requirement: to include the Risk Executive; 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Control Enhancement RA-5 (1)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

| RA-5 (1) | Control Enhancement 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)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement RA-5 (2)

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*FedRAMP* *Assignment: prior to a new scan*].

| RA-5 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement RA-5 (3)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| RA-5 (3) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| RA-5 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement RA-5 (5)

The organization includes privileged access authorization to [*FedRAMP Assignment: operating systems, databases, web applications*] for selected [*Assignment: all scans*].

| RA-5 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter RA-5(5)-1: | |
| Parameter RA-5(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement RA-5 (6)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

**RA-5(6) Additional FedRAMP Requirements and Guidance: Guidance:** Include in Continuous Monitoring ISSO digest/report to JAB

| RA-5 (6) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| RA-5 (6) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement RA-5 (8)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

**RA-5(8) Additional FedRAMP Requirements and Guidance:** **Requirement:** This enhancement is required for all high vulnerability scan findings.

**Guidance**: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

| RA-5 (8) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| RA-5 (8) What is the solution and how is it implemented? |
| --- |
|  |

System and Services Acquisition (SA)

System and Services Acquisition Policy and Procedures (SA-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [*FedRAMP Assignment: at least every three years*]; and
   2. System and services acquisition procedures [*FedRAMP Assignment: at least annually*].

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

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

Allocation of Resources (SA-2)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

System Development Life Cycle (SA-3)

The organization:

1. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Acquisitions Process (SA-4)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

**Additional FedRAMP Requirements and Guidance:** **Guidance:** The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See <http://www.niap-ccevs.org/vpl> or <http://www.commoncriteriaportal.org/products.html>.

| SA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 |  |

Control Enhancement SA-4 (1)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

| SA-4 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-4 (2)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*FedRAMP Selection: to include security-relevant external system interfaces and high-level design*]; [*Assignment: organization-defined design/implementation information*]] at [*Assignment: organization-defined level of detail*].

| SA-4 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-4-1: | |
| Parameter SA-4-2: | |
| Parameter SA-4-3: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-4 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-4 (8)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*FedRAMP Assignment: at least the minimum requirement as defined in control CA-7*].

**SA-4(8) Additional FedRAMP Requirements and Guidance:** Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

| SA-4 (8) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-4(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement SA-4 (9)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

| SA-4 (9) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-4 (9) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-4 (10)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| SA-4 (10) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
|  |

Information System Documentation (SA-5)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

| SA-5 | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-5(c): | |
| Parameter SA-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Security Engineering Principles (SA-8)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| SA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-8 What is the solution and how is it implemented? |
| --- |
|  |

External Information System Services (SA-9)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [*FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [*FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored]* to monitor security control compliance by external service providers on an ongoing basis.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement SA-9 (1)

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*FedRAMP Assignment: see Additional Requirement and Guidance*].

|  |  |
| --- | --- |
| SA-9 (1) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter SA-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

**SA-9 (1) Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.

| SA-9 (1) | Additional FedRAMP 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-9 (1) Additional: What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-9 (2)

The organization requires providers of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] to identify the functions, ports, protocols, and other services required for the use of such services.

|  |  |
| --- | --- |
| SA-9 (2) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter SA-9(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-9 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-9 (4)

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*FedRAMP Assignment: All external systems where Federal information is processed or store*] are consistent with and reflect organizational interests.

|  |  |
| --- | --- |
| SA-9 (4) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter SA-9(4)-1: | |
| Parameter SA-9(4)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-9 (4) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-9 (5)

The organization restricts the location of [*FedRAMP Selection: information processing, information data, AND information services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

|  |  |
| --- | --- |
| SA-9 (5) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter SA-9(5)-1: | |
| Parameter SA-9(5)-2: | |
| Parameter SA-9(5)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-9 (5) What is the solution and how is it implemented? |
| --- |
|  |

Developer Configuration Management (SA-10)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [*FedRAMP Selection: development, implementation, AND operation*];
2. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

**SA-10(e) Additional FedRAMP Requirements and Guidance: Requirement:** For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-10(a): | |
| Parameter SA-10(b): | |
| Parameter SA-10(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Control Enhancement SA-10 (1)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

| SA-10 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-10 (1) What is the solution and how is it implemented? |
| --- |
|  |

Developer Security Testing and evaluation (SA-11)

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SA-11(b)-1: | |
| Parameter SA-11(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Control Enhancement SA-11 (1)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

**SA-11 (1) Additional FedRAMP Requirements and Guidance:** **Requirement:** (Requirement for SA-11 (1) or SA-11 (8) or both)**:** The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-11 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-11 (2)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

| SA-11 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-11 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SA-11 (8)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

**SA-11 (8) Additional FedRAMP Requirements and Guidance:** **Requirement:** (Requirement for SA-11 (1) or SA-11 (8) or both): The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (8) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SA-11 (8) What is the solution and how is it implemented? |
| --- |
|  |

System and Communications Protection (SC)

System And Communications Protection Policy and Procedures (SC-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [*FedRAMP* *Assignment: at least every three years*]; and
   2. System and communications protection procedures [*FedRAMP Assignment: at least annually*].

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

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Application Partitioning (SC-2)

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-2 What is the solution and how is it implemented? |
| --- |
|  |

Information In Shared Resources (SC-4)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-4 What is the solution and how is it implemented? |
| --- |
|  |

Denial of Service Protection (SC-5)

The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

| SC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-5-1 | |
| Parameter: SC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-5 What is the solution and how is it implemented? |
| --- |
|  |

Resource Availability (SC-6)

The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

| SC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter: SC-6-1 | |
| Parameter: SC-6-2 | |
| Parameter: SC-6-3 | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-6 What is the solution and how is it implemented? |
| --- |
|  |

Boundary Protection (SC-7)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement SC-7 (3)

The organization limits the number external network connections to the information system.

| SC-7 (3) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-7 (4)

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [*FedRAMP Assignment: at least annually*] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(4)(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

Control Enhancement SC-7 (5)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| SC-7 (5) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-7 (7)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

| SC-7 (7) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (7) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-7 (8)

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

| SC-7 (8) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(8)(1): | |
| Parameter SC-7(8)(2): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (8) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-7 (12)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

| SC-7 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(12)-1 | |
| Parameter SC-7(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-7 (13)

The organization isolates [*FedRAMP* *Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

**SC-7 (13) Additional FedRAMP Requirements and Guidance:** The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

| SC-7 (13) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(13)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (13) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-7 (18)

The information system fails securely in the event of an operational failure of a boundary protection device.

| SC-7 (18) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
|  |

Transmission confidentiality and Integrity (SC-8)

The information system protects the [*FedRAMP Assignment: confidentiality AND integrity*] of transmitted information.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-8 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-8 (1)

The information system implements cryptographic mechanisms to [*FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information*] during transmission unless otherwise protected by [*FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)*].

| SC-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-8(1)-1: | |
| Parameter SC-8(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Network Disconnect (SC-10)

The information system terminates the network connection associated with a communications session at the end of the session or after [*FedRAMP Assignment:*  *no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions*] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-10 What is the solution and how is it implemented? |
| --- |
|  |

Cryptographic Key Establishment & Management (SC-12)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

**SC-12 Additional FedRAMP Requirements and Guidance**: **Guidance:** Federally approved cryptography

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-12 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-12 (2)

The organization produces, controls, and distributes symmetric cryptographic keys using [*FedRAMP* *Selection: NIST FIPS-compliant*] key management technology and processes.

| SC-12 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-12 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-12 (3)

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key*].

| SC-12 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-12(3): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-12 (5) What is the solution and how is it implemented? |
| --- |
|  |

Use of Cryptography (SC-13)

The information system implements [*FedRAMP Assignment:* *FIPS-validated or NSA-approved cryptograph]* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-13: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-13 What is the solution and how is it implemented? |
| --- |
|  |

Collaborative Computing Devices (SC-15)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[*FedRAMP Assignment: no exceptions*] and
2. Provides an explicit indication of use to users physically present at the devices.

| SC-15 | 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

**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 | Additional 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 |  |

Public Key Infrastructure Certificates (SC-17)

The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*]or obtains public key certificates from an approved service provider.

| SC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SC-17: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-17 What is the solution and how is it implemented? |
| --- |
|  |

Mobile Code (SC-18)

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Voice Over Internet Protocol (SC-19)

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Secure Name-Address Resolution Service (Authoritative Source) (SC-20)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

| SC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-21 What is the solution and how is it implemented? |
| --- |
|  |

Architecture and Provisioning for Name-Address Resolution Service (SC-22)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-22 What is the solution and how is it implemented? |
| --- |
|  |

Session Authenticity (SC-23)

The information system protects the authenticity of communications sessions.

| SC-23 | 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-23 What is the solution and how is it implemented? |
| --- |
|  |

Protection of Information At Rest (SC-28)

The information system protects the [*FedRAMP* *Selection: confidentiality AND integrity]*] of [*Assignment: organization-defined information at rest*].

**SC-28 Additional FedRAMP Requirements and Guidance:** **Requirement:** The organization supports the capability to use cryptographic mechanisms to protect information at rest.

| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-28 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SC-28 (1)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*]

| SC-28 (1) | Control Enhancement 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:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-28 (1) What is the solution and how is it implemented? |
| --- |
|  |

Process Isolation (SC-39)

The information system maintains a separate execution domain for each executing 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-39 What is the solution and how is it implemented? |
| --- |
|  |

System and Information Integrity (SI)

System & Information Integrity Policy & Procedures (SI-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
   1. System and information integrity policy [*FedRAMP* *Assignment: at least every three years*]; and
   2. System and information integrity procedures [*FedRAMP Assignment: at least annually*].

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

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Flaw Remediation (SI-2)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [*FedRAMP* *Assignment: Within 30 days of release of updates*] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement SI-2 (2)

The organization employs automated mechanisms [*FedRAMP Assignment: at least monthly*] to determine the state of information system components with regard to flaw remediation.

| SI-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement SI-2 (3)

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

| SI-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-2(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-2 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Malicious Code Protection (SI-3)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [*FedRAMP Assignment: at least weekly*] and real-time scans of files from external sources at [*FedRAMP Assignment to include endpoints*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [*FedRAMP Assignment: to include alerting administrator or defined security personnel*] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-3(c)(1)-1: | |
| Parameter SI-3(c)(1)-2 | |
| Parameter SI-3(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Control Enhancement SI-3 (1)

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-3 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-3 (2)

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-3 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-3 (7)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SC-3 (7) What is the solution and how is it implemented? |
| --- |
|  |

Information System Monitoring (SI-4)

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
3. Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

| SI-4 | 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| 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 |  |

Control Enhancement SI-4 (1)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| SI-4 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-4 (2)

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-4 (4)

The information system monitors inbound and outbound communications traffic [*FedRAMP Assignment:* *continually]* for unusual or unauthorized activities or conditions.

| SI-4 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-4(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-4 (5)

The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

**SI-4(5) Additional FedRAMP Requirements and Guidance:** **Guidance:** In accordance with the incident response plan.

| SI-4 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-4(5)-1: | |
| Parameter SI-4(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (5) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-4 (14)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

| SI-4 (14) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-4 (16)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-4 (23)

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

| SI-4 (23) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-4(23)-1: | |
| Parameter SI-4(23)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-4 (23) What is the solution and how is it implemented? |
| --- |
|  |

Security Alerts & Advisories (SI-5)

The organization:

1. Receives information system security alerts, advisories, and directives from [*FedRAMP Assignment : to include US-CERT*] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [*FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities*]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

Security Functionality Verification (SI-6)

The information system:

1. Verifies the correct operation of [*Assignment: organization-defined security functions*];
2. Performs this verification [*FedRAMP Assignment: to include upon system startup and/or restart at least monthly*
3. Notifies [*FedRAMP Assignment: to include system administrators and security personnel*] of failed security verification tests; and
4. [*Selection (one or more): shuts the information system down; restarts the information system;* [*FedRAMP Assignment: to include notification of system administrators and security personnel*] when anomalies are discovered.

| SI-6 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-6(a): | |
| Parameter SI-6(b): | |
| Parameter SI-6(c) | |
| Parameter SI-6(d)-1 | |
| Parameter SI-6(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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Software & Information Integrity (SI-7)

The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

| SI-7 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-7: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-7 What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-7 (1)

The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*FedRAMP Selection (one or more): at startup; at* [*FedRAMP Assignment: to include security-relevant events*]; [*FedRAMPAssignment: at least monthly*]].

| SI-7 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-7(1)-1: | |
| Parameter SI-7(1)-2: | |
| Parameter SI-7(1)-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement SI-7 (7)

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

| SI-7 (7) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-7(7): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-7 (7) What is the solution and how is it implemented? |
| --- |
|  |

Spam Protection (SI-8)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

| SI-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Control Enhancement SI-8 (1)

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

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

Control Enhancement SI-8 (2)

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Enhancement 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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

|  |
| --- |
| SI-8 (2) What is the solution and how is it implemented? |
|  |

Information Input Validation (SI-10)

The information system checks the validity of [*Assignment: organization-defined information inputs*].

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-10 What is the solution and how is it implemented? |
| --- |
|  |

Error Handling (SI-11)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [*Assignment: organization-defined personnel or roles*]

| SI-11 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |

Information Output Handling and Retention (SI-12)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| SI-12 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-12 What is the solution and how is it implemented? |
| --- |
|  |

Memory Protection (SI-16)

The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter SI-16 | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| SI-16 What is the solution and how is it implemented? |
| --- |
|  |

Acronyms

| Acronym | Definition |
| --- | --- |
| 3PAO | Third Party Assessment Organization |
| ATO | Authority To Operate |
| CONOPS | Concept Of Operations |
| CSP | Cloud Service Provider |
| DHS | Department of Homeland Security |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standard |
| GSA | General Services Administration |
| ISSO | Information System Security Officer |
| JAB | Joint Authorization Board |
| NARA | National Archives and Records Administration |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PII | Personally Identifiable Information |
| PMO | Program Management Office |
| POA&M | Plan Of Action & Milestones |
| SAP | Security Assessment Plan |
| SLA | Service Level Agreement |
| SOC | Security Operations Center |
| SSP | System Security Plan |
| US-CERT | U.S. Computer Emergency Response Team |

SYSTEMS SECURITY PLAN ATTACHMENTS

*Instruction: Attach any documents that are referred to in the <Information System Name> System Security Plan. Documents may be attached as an embedded file or if the file is not embedded and is sent to FedRAMP by other means, provide the title, version, and exact file name, including the file extension.*

1. ATTACHMENT 1 - [Information Security Policies]
2. ATTACHMENT 2 - [User Guide]
3. ATTACHMENT 3 - [e-Authentication Worksheet]
4. ATTACHMENT 4 - [PTA/PIA]
5. ATTACHMENT 5 - [Rules of Behavior]
6. ATTACHMENT 6 - [IT Contingency Plan]
7. ATTACHMENT 7 - [Configuration Management Plan]
8. ATTACHMENT 8 - [Incident Response Plan]
9. ATTACHMENT 9 - [CIS Workbook]