FedRAMP System Security Plan (SSP) Moderate Baseline Template

Cloud Service Provider Name

Information System Name

Version #

Version Date

FedRAMP

Instruction: This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.

Repeatable Field

Some multiple-occurring data fields have been linked together and you need only enter the data once. Enter the data once; then click outside the data entry field and all occurrences of that field will be populated. For example, when you see "Information System Abbreviation" and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:

CSP Name
Information System Name
Version Number
Version Date
Information System Abbreviation

If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes. The one exception to the repeatable fields is information system names for FedRAMP or leveraged authorizations that are identified as "Leveraged information system name:

Date Selection

Data fields that must contain a date will present a date selection menu.

Item Choice

Data fields that have a limited number of value choices will present a selection list.

Number Entry

Data fields that must have numeric values display "number."

Text Entry

Many data fields, particularly in tables, that can contain any text display "Enter text" or "Click here to enter text."

Delete this instruction from your final version of this document.

System Security Plan

Prepared by

Identification of Organization that Prepared this Document		
	Organization Name	<Entermpany/Organization>.
	Street Address	<Enter Street Address>
	Suite/Room/Building	<Enter Suite/Room/Building>
	City, State Zip	<Enter Zip Code>

Prepared for

Identification of Cloud Service Provider		
	Organization Name	<Enter Company/Organization>.
	Street Address	<Enter Street Address>
	Suite/Room/Building	<Enter Suite/Room/Building>
	City, State Zip	<Enter Zip Code>

Template Revision History

Date	Description
1/21/2013	Original publication
6/6/2014	Major revision for SP800-53 Revision 4. Includes new template and formatting changes.
6/6/2018	Revised controls for language consistency and updated Attachment 3

Date	Description
6/20/2016	Reformatted to FedRAMP Document Standard, added repeated text schema and content fields to tables that were not Control Tables. Revised cover page, changed document designation to Controlled Unclassified Information (CUI), Removed front matter section How This Document is Organized, Instructions re-written, Corrected section numbering to match SSP v1.0, Revised Section 9 Table 9-1 Personnel Roles and Privileges, Removed Section 10 inventory tables (see Attachment 13 FedRAMP Inventory Workbook). Global verbiage change, Authorizing Official (AO) changed to JAB/AO; e-Authentication, e-authentication and E-authentication changed to E-Authentication. Added attachments 10 FIPS 199, 11 Separation of Duties Matrix, 12 FedRAMP Laws and Regulations, 13 FedRAMP Inventory Workbook. Changes to the following controls: AC-02 (05), AC-05, AC-17 (09), AU-03 (01), AU-05, AU-06, CA-02 (03), CA-7, CM-02 (01), IA-02 (11), MP-03, PL-08, SA-09 (01), SC-15, SI-04 (04)
10/21/2016	Removed tables in Sec 15.12 FedRAMP Laws and Regulations Removed revision history tables in all of Sec 15 Removed Acronyms - see FedRAMP Master Acronyms and Glossary resource document Added PTA to Sec 15.4 PTA and PIA Added E-Authentication to Sec 15.3 Added FIPs to Sec 15.10 FIPS 199 Changed Inventory instruction and guidance Sec 10 and Attachment 13 Removed chapter numbers from Attachments Removed 3 questions from Sec 2.3 E-Authentication Determination
3/6/2017	Document renamed from "FedRAMP System Security Plan (SSP) Moderate Baseline Master Template to "FedRAMP System Security Plan (SSP) Moderate Baseline Template”
6/6/2017	Updated logo
8/28/2018	Revised controls for language consistency, updated section 2.3 and Attachment 3, added guidance to SA -9, updated requirements in RA-5
5/18/2021	Revised SA-4 Additional FedRAMP Requirements and Guidance

Document Revision History

Date	Description	Version of SSP	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to contact us

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

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

Instruction: The System Security Plan is the main document in which the Cloud Service Provider (CSP) describes all the security controls in use on the information system and their implementation.

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

This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).

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 described in some way by the service provider.
*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

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 System as a Service (SaaS) and Platform as a Service (PaaS) systems that are inheriting controls from an Infrastructure as a Service (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 National Institute of Standards and Technology (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.

Delete this instruction from your final version of this document.

TABLE OF CONTENTS

List of Figures

List of Tables

System Security Plan Approvals

Cloud Service Provider Signatures

Name <Enter Name> Date <Select Date>

Title <Enter Title>

Cloud Service Provider CSP Name

Name <Enter Name> Date <Select Date>

Title <Enter Title>

Cloud Service Provider CSP Name

Name <Enter Name> Date <Select Date>

Title <Enter Title>

Cloud Service Provider CSP Name

1. Information System Name/Title

This System Security Plan provides an overview of the security requirements for the Information System Name (Enter 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 Enter Information System Abbreviation information system.

The security safeguards implemented for the Enter 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.

Table 1-1. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
<Enter FedRAMP Application Number>	Information System Name	Enter Information System Abbreviation

2. Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2-1 Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: ATTACHMENT 10 - FIPS 199.

Table 2-1. Security Categorization

System Sensitivity Level:	Choose level.

2.1. 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 Enter Information System Abbreviation. The selection of the information types is based on guidance provided by Office of Management and Budget (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 Special Publication (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: Record your information types in the tables that follow. Record the sensitivity level 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.

Delete this instruction from your final version of this document.

Example:

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

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
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2 Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, default to the high-water mark for the Information Types as identified in Table 2-3 Security Impact Level below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	Choose level.
Integrity	Choose level.
Availability	Choose level.

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 2-4 Baseline Security Configuration that follows.

Table 2-4. Baseline Security Configuration

Enter Information System Abbreviation Security Categorization	Choose level

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.

2.3. Digital Identity Determination

The digital identity information may be found in ATTACHMENT 3 – Digital Identity Worksheet

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

Additional digital identity information can be found in Section 15 Attachments Digital Identity Level Selection.

3. Information System Owner

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

Table 3-1. Information System Owner

Information System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4. Authorizing Official

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

JAB P-ATO: FedRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS)

Agency Authority to Operate (ATO): Agency Authorizing Official name, title and contact information

Delete this and all other instructions from your final version of this document.

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

5. Other Designated Contacts

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

Delete this and all other instructions from your final version of this document.

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

Table 5-1. Information System Management Point of Contact

Information System Management Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 5-2. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.

Information System Technical Point of Contact	
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

6. 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.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

7. Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7-1 System Status that follows. (Only operational systems can be granted an ATO).

Table 7-1. System Status

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: Click here to enter text.

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

Delete this and all other instructions from your final version of this document.

8. Information System Type

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

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1 Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table 8-1. Service Layers Represented in this SSP

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: Click here to enter text.

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

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2 Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

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

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
☐	Government Only 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) Click here to enter text.

8.3. 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. 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.

Delete this and all other instructions from your final version of this document.

The Enter Information System Abbreviation Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Enter Information System Abbreviation are listed in Table 8-3 Leveraged Authorizations that follows.

Table 8-3. Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
<Enter Leveraged information system name1>	<Enter service provider owner1>	<Date>
<Enter Leveraged information system name2>	<Enter service provider owner2>	<Date>
<Enter Leveraged information system name3>	<Enter service provider owner3>	<Date>

9. General System Description

This section includes a general description of the Enter Information System Abbreviation.

9.1. System Function or Purpose

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

Delete this and all other instructions from your final version of this document.

9.2. Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system's Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].

Additional FedRAMP Requirements and Guidance:

Guidance: *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1 Authorization Boundary Diagram below.

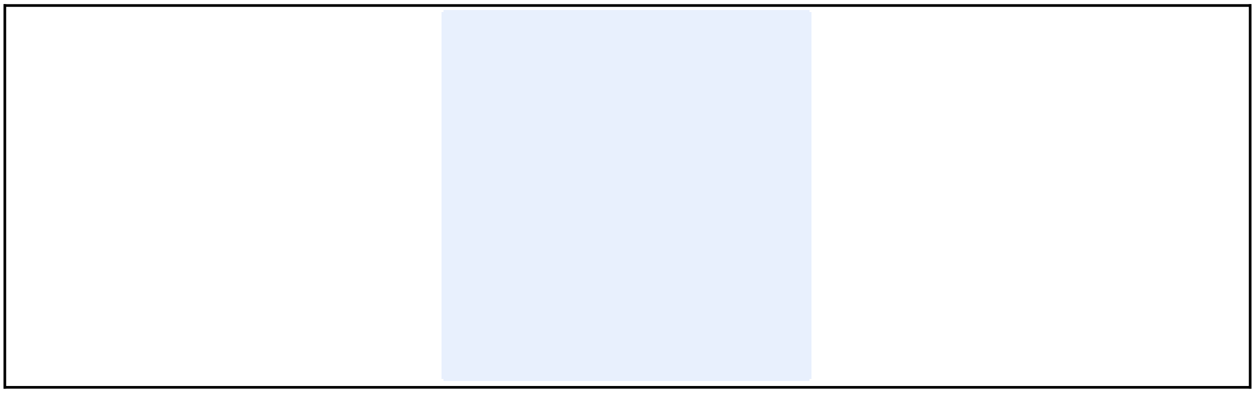

Figure 9-1 Authorization Boundary Diagram

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (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 Table 9-1 Personnel Roles and Privileges that follows.

Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles 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.

Delete this and all other instructions from your final version of this document.

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

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

9.4. Network Architecture

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

Delete this and all other instructions from your final version of this document.

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

The logical network topology is shown in Figure 9-2 Network Diagram mapping the data flow between components.

The following Figure 9-2 Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.

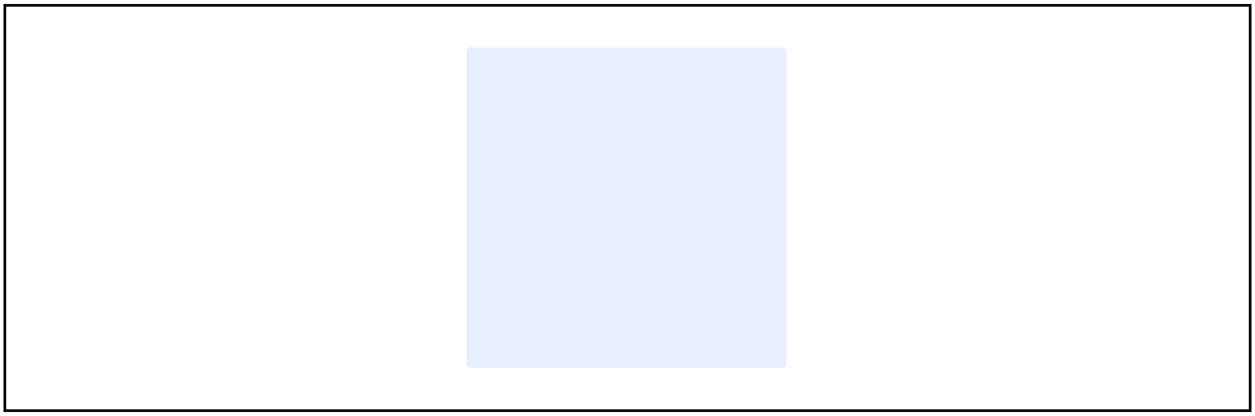

Figure 9-2 Network Diagram

10. System Environment And Inventory

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: ATTACHMENT 13 – FedRAMP Inventory Workbook.

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 the specific location of the alternate, backup and operational facilities.

In your description, also include a reference to Attachment 13, the system's Integrated Inventory Workbook, which should provide a complete listing of the system's components (operating systems/infrastructure, web applications/software, and databases). The Integrated Inventory Workbook should be maintained and updated monthly by the CSP, as part of continuous monitoring efforts. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook.

Delete this and all other instructions from your final version of this document.

10.1. 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. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

The data flow in and out of the system boundaries is represented in Figure 10-1 Data Flow Diagram below.

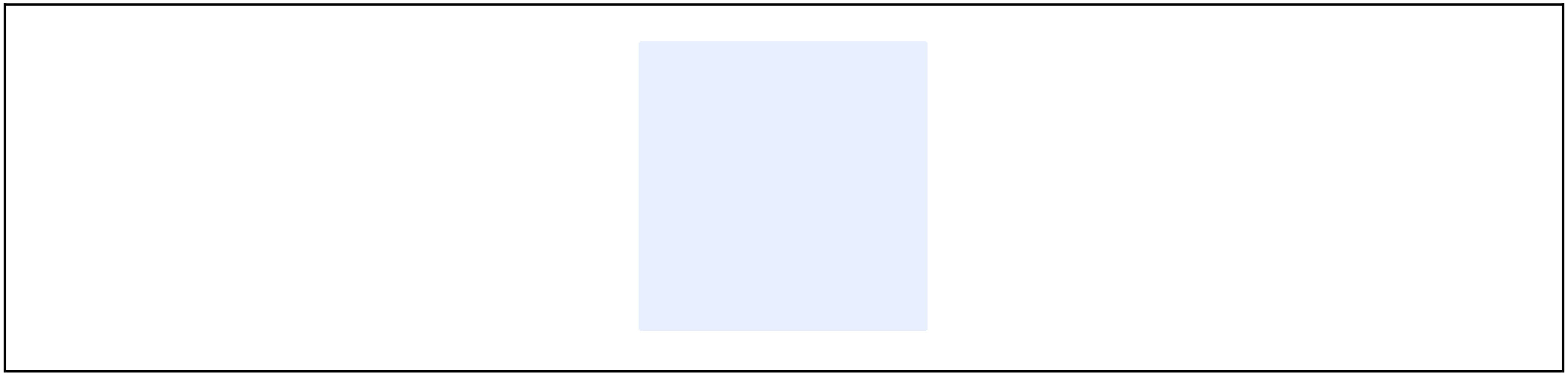

Figure 10-1 Data Flow Diagram

10.2. Ports, Protocols and Services

Table 10-1 Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled "Used By" please 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 should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.

Delete this and all other instructions from your final version of this document.

Table 10-1 Ports, Protocols and Services

Ports (TCP/UDP)*	Protocols	Services	Purpose	Used By
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>

* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

11. 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. Provide a point of contact and phone number for the external organization. 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 Table 13-3 CA-3 Authorized Connections.

Additional FedRAMP Requirements and Guidance:

***Guidance:** See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/
Delete this and all other instructions from your final version of this document.

The Table 11-1 System Interconnections below is consistent with Table 13-3 CA-3 Authorized Connections.

Table 11-1. System Interconnections

SP* 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	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

SP* 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	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

*Service Processor

**Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

12. Laws, Regulations, Standards and Guidance

A summary of FedRAMP Laws and Regulations is included in ATTACHMENT 12 – FedRAMP Laws and Regulations.

12.1. Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: Templates.

Table 12-1 Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional laws and regulations that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table 12-1. Information System Name Laws and Regulations

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

12.2. Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: Templates

Table 12-2 Information System Name Standards and Guidance includes in this section any additional standards and guidance specific to Information System Name.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional standards or guidance that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table 12-2. Information System Name Standards and Guidance

Identification Number	Title	Date	Link
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>
<Reference ID>	<Reference Title>	<Ref Date>	<Reference Link>

13. 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 corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of Enter 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 parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13-1 Summary of Required Security Controls that follows.

Table 13-1. Summary of Required Security Controls

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
AC	**Access Control**			
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4 (21)	AC-4 (8) (21)
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (7) (8) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7 (2)
AC-8	System Use Notification	AC-8	AC-8	AC-8

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
AC-10	Concurrent Session Control	Not Selected	AC-10	AC-10
AC-11	Session Lock	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-14	Permitted Actions Without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)
AC-18	Wireless Access	AC-18	AC-18 (1)	AC-18 (1) (3) (4) (5)
AC-19	Access Control For Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22
AT	**Awareness and Training**			
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	AT-3	AT-3	AT-3 (3) (4)
AT-4	Security Training Records	AT-4	AT-4	AT-4
AU	**Audit and Accountability**			
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis and Reporting	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (4) (5) (6) (7) (10)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (2) (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12 (1) (3)
CA	**Security Assessment and Authorization**			
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1) (2) (3)	CA-2 (1) (2) (3)
CA-3	System Interconnections	CA-3	CA-3 (3) (5)	CA-3 (3) (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
CA-7	Continuous Monitoring	CA-7	CA-7 (1)	CA-7 (1) (3)
CA-8	Penetration Testing	Not Selected	CA-8 (1)	CA-8 (1)
CA-9	Internal System Connections	CA-9	CA-9	CA-9
CM	**Configuration Management**			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (2) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (1) (2) (4) (6)
CM-4	Security Impact Analysis	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions For Change	Not Selected	CM-5 (1) (3) (5)	CM-5 (1) (2) (3) (5)
CM-6	Configuration Settings	CM-6	CM-6 (1)	CM-6 (1) (2)
CM-7	Least Functionality	CM-7	CM-7 (1) (2) (5)*	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10 (1)	CM-10 (1)
CM-11	User-Installed Software	CM-11	CM-11	CM-11 (1)
*FedRAMP does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented.				
CP	**Contingency Planning**			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (3)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2)	CP-10 (2) (4)
IA	**Identification and Authentication**			
IA-1	Identification and Authentication Policy and Procedures	IA-1	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-2 (1) (2) (3) (4) (5) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4 (4)	IA-4 (4)
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)	IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IR	**Incident Response**			
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1) (2) (3) (4) (6) (8)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1) (2)	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	Not Selected	IR-9 (1) (2) (3) (4)	IR-9 (1) (2) (3) (4)
MA	**Maintenance**			
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	Not Selected	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (2)	MA-4 (2) (3) (6)
MA-5	Maintenance Personnel	MA-5	MA-5 (1)	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
MP	**Media Protection**			
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2
MP-3	Media Marking	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6 (2)	MP-6 (1) (2) (3)
MP-7	Media Use	MP-7	MP-7 (1)	MP-7 (1)
PE	**Physical and Environmental Protection**			
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control For Transmission Medium	Not Selected	PE-4	PE-4
PE-5	Access Control For Output Devices	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (4)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
PE-8	Visitor Access Records	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14 (2)	PE-14 (2)
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	Not Selected	PE-18
PL	**Planning**			
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2 (3)	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4 (1)	PL-4 (1)
PL-8	Information Security Architecture	Not Selected	PL-8	PL-8
PS	**Personnel Security**			
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3 (3)	PS-3 (3)
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
RA	**Risk Assessment**			
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-5	Vulnerability Scanning	RA-5	RA-5 (1) (2) (3) (5) (6) (8)	RA-5 (1) (2) (3) (4) (5) (6) (8) (10)
SA	**System and Services Acquisition**			
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3
SA-4	Acquisition Process	SA-4 (10)	SA-4 (1) (2) (8) (9) (10)	SA-4 (1) (2) (8) (9) (10)
SA-5	Information System	SA-5	SA-5	SA-5

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
	Documentation			
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9 (1) (2) (4) (5)	SA-9 (1) (2) (4) (5)
SA-10	Developer Configuration Management	Not Selected	SA-10 (1)	SA-10 (1)
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11 (1) (2) (8)	SA-11 (1) (2) (8)
SA-12	Supply Chain Protection	Not Selected	Not Selected	SA-12
SA-15	Development Process, Standards and Tools	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected	SA-17
SC	**System and Communications Protection**			
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information In Shared Resources	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Availability	Not Selected	SC-6	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)	SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8 (1)	SC-8 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12 (2) (3)	SC-12 (1) (2) (3)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name / Address Resolution Service	SC-22	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23 (1)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
SC-24	Fail in Known State	Not Selected	Not Selected	SC-24
SC-28	Protection of Information At Rest	Not Selected	SC-28 (1)	SC-28 (1)
SC-39	Process Isolation	SC-39	SC-39	SC-39
SI	**System and Information Integrity**			
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2) (3)	SI-2 (1) (2) (3)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2) (7)	SI-3 (1) (2) (7)
SI-4	Information System Monitoring	SI-4	SI-4 (1) (2) (4) (5) (14) (16) (23)	SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24)
SI-5	Security Alerts, Advisories and Directives	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	Not Selected	SI-6	SI-6
SI-7	Software, Firmware and Information Integrity	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-10	Information Input Validation	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12
SI-16	Memory Protection	SI-16	SI-16	SI-16

Note: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

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.

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.

Please note: CSPs should not modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements. CSP responses must be documented in the "Control

Summary Information" and "What is the solution and how is it implemented?" tables.

Delete this and all other instructions from your final version of this document.

The definitions in Table 13-2. Control Origination and Definitions indicate where each security control originates.

Table 13-2. Control Origination and Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP Name 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 Name 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 Name.	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 Name and partially by the customer.	Security awareness training must be conducted by both the CSPN and the customer.
Inherited from pre-existing FedRAMP Authorization	A control that is inherited from another CSP Name system that has already received a FedRAMP Authorization.	A PaaS or SaaS provider inherits PE controls from an IaaS provider.

*Hyper Text Transport Protocol (http)

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

13.1. Access Control (AC)

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

The organization:

(a) Develops, documents and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

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 b1	

AC-1 What is the solution and how is it implemented?	
Part b2	

AC-2 Account Management (L) (M)

The organization:

(a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

(b) Assigns account managers for information system accounts;

(c) Establishes conditions for group and role membership;

(d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

(e) Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

(f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

(g) Monitors the use of information system accounts;

(h) Notifies account managers:

(1) When accounts are no longer required;

(2) When users are terminated or transferred; and

(3) When individual information system usage or need-to-know changes;

(i) Authorizes access to the information system based on:

(1) A valid access authorization;
(2) Intended system usage; and
(3) Other attributes as required by the organization or associated missions/business functions;

(j) Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and

(k) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

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

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

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

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

AC-2 (2) Control Enhancement (M)

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

AC-2 (2)	Control Summary Information
Responsible Role:	
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)	

AC-2 (2)	Control Summary Information
☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-2 (3) Control Enhancement (M)

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

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

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

AC-2 (3)	Control Enhancement Summary Information
Responsible Role:	
Parameter AC-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-2 (4) Control Enhancement (M)

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

AC-2 (4)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-2 (5) Control Enhancement (M)

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

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

Guidance: Should use a shorter timeframe than AC-12

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

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

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

AC-2 (7) Control Enhancement (M)

The organization:

(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;

Monitors privileged role assignments; and

Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.

AC-2 (7)	**Control 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	

AC-2 (7)	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-2 (9) Control Enhancement (M)

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

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

AC-2 (9)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

AC-2 (12) Control Enhancement (M)

The organization:

(a) Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and

Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

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

AC-2 (12)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

AC-3	Control Summary Information
Responsible Role: Accounts Manager	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

AC-3	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-3 What is the solution and how is it implemented?
The account management department monitors all the accounts and the activities from every account. Whenever a request for account creation arrives to account management department with specific resources accesses, the department reviews the requests and tallies it with the control policies and standards mentioned in the documentation and provides approval only if all the standards are satisfied. If any account requires some extra access to some resources and system for a specific period of time, the request is also sent to account manager, who would review the access for any security threats and ensures if it is in accordance with the control policies. The approval is provided after the scrutiny. The approvals may be generated on the basis of some conditions, for instance, just read only access to a database for generating reports using the software and it can only be accessed within a particular duration in a day. After the end of the required period, the access is revoked. The account will be locked if there is more than 3 attempts to access an unauthorized resource and system, and it will be notified to the account manager. The account will be unlocked only after thorough review of the action performed from the account. The account manager also ensures that no unused individual or group accounts are active. It also makes sure that no unauthorized individual account access a group account even with correct credentials.

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

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

AC-4	Control Summary Information
Responsible Role: Information infrastructure Manager	
Parameter AC-4: Well encapsulated information access policy	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

AC-4	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ✅ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-4 What is the solution and how is it implemented?
A well encapsulated information flow system ensures that the information is available for the users only if they have privileges to access it. This can be overturned in cases of emergency, special use cases, temporary privileges and so on.The idea here is to allow the departments to keep their confidentiality for themselves, ofcourse this does not incur department managers and directors who have a master key to tap into the information flow if they need to. To double down on this , we are also planning limit these privileges of managers and directors by granting them the same for over a limited period of time upon request. This would allow a great balance of security and flexibility for a secure and efficient operation, maintenance and development within the system.

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

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

AC-4 (21)	Control Summary Information
Responsible Role: Information Security Team	
Parameter AC-4(21)-1: User account based information flow	
Parameter AC-4(21)-2: Information flow with respect to the relevant department	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-4 (21) What is the solution and how is it implemented?
The System separates the information flows logically among the teams with respect to the relevance of the information to the corresponding teams. This way the system can restrict unwanted information leaks among various entities with in the organization. This logic works with the nature of information, for example, real time information, biological information , criminal history, logistical information etc and the teams which govern over or work with the said information.

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

The organization:

(a) Separates [*Assignment: organization-defined duties of individuals*];

(b) Documents separation of duties of individuals; and

(c) Defines information system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Section 15.11 ATTACHMENT 11 - Separation of Duties Matrix.

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-6 Least Privilege (M) (H)

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

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

AC-6 What is the solution and how is it implemented?
The Information Security Manager maintains the lowest possible permission level when users are accessing the data that we are concerned - Parolee's day-to-day activities. Uers are granted permissions to read,write or execute only for certain files and folders. Suppose there is a threat detected in the system, the process from that point onwards will be blocked from picking up on critical process that houses all the data. The system is only allowed to do only the basic process that keeps the system running. Since the duties are defined among the users, any tasks that are not in the scope of specific user's duty will be revoked. Each duty will be given only the permission levels that are required to execute their tasks. If the user tries to access the restricted content the system logs this attempt and it is later taken for the audit. The Information Security Manager authenticate the user that is seeking to receive the permission, by checking all their background and credentials. They will be then authorized by granting what actions they are allowed to perform. Their access is monitored to see their usage patterns.

AC-6 (1) Control Enhancement (M)

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

AC-6 (1) What is the solution and how is it implemented?
The role of the user scope being limited to their specific duty will not need access to other operations, hence they are not allowed to access restricted data.

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

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 non-security functions.

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

AC-6 (2)	**Control Summary Information**
Responsible Role: Information Security Manager	
Parameter AC-6(2): Logistic and organisational processes	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Date of Authorization ,	

AC-6 (2) What is the solution and how is it implemented?
The critical functionalities have to be having highest privilege levels. The functions that do not involve high critical tasks should be allowed to use non-security accounts in-order to carry such low security tasks.

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

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

AC-6 (5)	**Control Summary Information**
Responsible Role: Information Security Manager	
Parameter AC-6 (5): Information Security Manager	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)	

AC-6 (5)	Control Summary Information
☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-6 (5) What is the solution and how is it implemented?
All levels of privileges - low to high, are handled by the information security manager. The manager decides which user has to receive what level of privilege access depending on the task they are assigned.

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

The information system audits the execution of privileged functions.

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

AC-6 (9) What is the solution and how is it implemented?
After the privilege levels for all the users have been assigned, an Internal auditing is carried out to check if the implementation is in compliance or not. This would be a one time auditing, after the privilege levels are assigned.

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

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

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

AC-6 (10) What is the solution and how is it implemented?
Non-privileged user functionalities are restricted from using critical data and processes of the system. Once the user responsibility and the scope is known to the system, anything that is beyond that scope is blocked from being used by the non-privileged user.

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

The organization:

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

Automatically [*Selection: locks the account/node for a* [*FedRAMP Assignment: thirty (30) minutes*]; *delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

AC-7	Control Summary Information
Responsible Role: Security Analyst	
Parameter AC-7(a)-1: Organisation Defined Number: 3	
Parameter AC-7(a)-2: Defined Time Period: 24 hours	
Parameter AC-7(b)-1: Locked for 24 hours	
Parameter AC-7(b)-2: Delay Algorithm	

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

AC-7 What is the solution and how is it implemented?	
Part a	Security analyst is responsible for the monitoring the network, investigate & make a report for the suspicious login into the network. Important aspect is to securing user's personal accounts and information. As per the organisation's predefined policies the login limit that is 3 unsuccessful login, if someone tried to login into system and if login attempts goes beyond the limit, the account will lock for 24 hours. This is to make it harder for the potential attackers to compromise the accounts, decrease the likelihood of the attack on the organisation's network.
Part b	After an unsuccessful login attempt threshold is exceeded and the system locks an account, the account may either remain locked until an administrator takes action to unlock it after checking with their respective IDs, or it may be locked for a predefined time after which it unlocks automatically.The account will be locked for 24 hours and once its completed the account will be unlocked automatically. This done using Delay Algorithm which show all the users who has logged in at unusual times and from unusual places.

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

The information system:

(a) Displays to users [*Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: 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;

(a) 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

For publicly accessible systems:

Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;
Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

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

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

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

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

AC-8	Control Summary Information
Responsible Role:	
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	

AC-8	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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/AO.

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/AO. 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/AO.

AC-8 Req.	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

AC-8 Req.	Control Summary Information
☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*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-10-1:	
Parameter AC-10-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-11 Session Lock (M) (H)

The information system:

(a) Prevents further access to the system by initiating a session lock after [*FedRAMP Assignment: fifteen (15) minutes*] of inactivity or upon receiving a request from a user; and

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

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

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

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

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

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

AC-12 Session Termination (M) (H)

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 Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)	

AC-12	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

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

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

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

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

The organization:

(a) Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

(b) Authorizes remote access to the information system prior to allowing such connections.

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

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

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

The information system monitors and controls remote access methods.

AC-17 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

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

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

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

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

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

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

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

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

AC-17 (3)	Control Summary Information
Responsible Role:	
Parameter AC-17(3):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Documents the rationale for such access in the security plan for the information system.

AC-17 (4)	Control 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 ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

AC-17 (9)	Control Summary Information
Responsible Role:	
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)	

AC-17 (9)	Control Summary Information
☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

(b) Authorizes wireless access to the information system prior to allowing such connections.

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

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

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

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

AC-18 (1)	**Control Summary Information**
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

(b) Authorizes the connection of mobile devices to organizational information systems.

AC-19	**Control Summary Information**
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

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

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

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

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

AC-19 (5)	Control Summary Information
Responsible Role:	
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 ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

(a) Access the information system from external information systems; and

(b) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

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

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

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

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

AC-20 (2)	Control Summary Information
Responsible Role:	

AC-20 (2)	Control Summary Information
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AC-21 Information Sharing (M) (H)

The organization:

(a) Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

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

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	

AC-21	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Designates individuals authorized to post information onto a publicly accessible information system;

(b) Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

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

(d) Reviews the content on the publicly accessible information system for nonpublic information [*FedRAMP Assignment: at least quarterly*] and removes such information, if discovered.

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

AC-22	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

13.2. Awareness and Training (AT)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

(b) Reviews and updates the current:

(1) Security awareness and training policy [*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: Security Enhancement Officer	

AT-1	Control Summary Information
Parameter AT-1(a): Documentation Expert and Security Enhancement Officer	
Parameter AT-1(b)(1): Every 3 years	
Parameter AT-1(b)(2): Anually	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific)	

AT-1 What is the solution and how is it implemented?	
Part a	The Security Enhancement Officer develops the policies and procedures to secure the control of the system by each account type and the ways of control enhancements. These policies include that from every individual account only one login from a single device is permitted at a time. If there is an attempt to login from more than one device, the login should be reported to the accounts manager. For every account type, even for the accounts from the CSP will have secure public and private keys to access the system and databases. In order to access the database, the privilege will only be given to Managers, Biological department, and monitoring accounts. The databases will only be accessed while in VPN. The policies will also include the trainings that include what resources can be accessed from each account, rules for accessing the systems like 2 step authentication for login, changing the password every 3 months, etc. The policies will be Pivotal Application Service compliant. After drafting the policies, the documentation expert frames the policies and procedures in a document that will be shared to all the account types. The procedures would include on how to implement the security awareness. The Security trainer will be assigned and they should be trained personally by security enhancement officer. Every user of the system will be shared a mandatory security training course which should be completed within 1 week of their account creation. The training courses can be online managed by IT Security team and by assigned Security trainers. After completion of the training, all the users have to go through a Q/A test and have to pass with 90% to get proper access to the system resources. In cases of failures for 3 repetitive attempts, the account will be locked and a show cause would be generated. These training courses will have all steps to set up their encrypted access to the system, specify what privileges they have and how they should follow basic security precautions. It will also include what steps to follow for emergency accounts to access the system.
Part b	The users have to report issues, potential threats and potential breaches with in the security system. The Security Enhancement officer can review the report based on their criticality and ensure to address them via a newsletter or mandatory training sessions if they need mandatory addressing. The Officer can then compile these reports into the organization's training policy. The officers have to train the trainer with the modification in procedures and explain them what things get unnoticed which caused the threat or breach and what measures have to taken to ensure its rectification. Then all the procedures are modified to incorporate those changes. Even if there is no issue, a screening is being carried out annually to check the security of the system and changes are incorporated in

AT-1 What is the solution and how is it implemented?	
	policies and procedures to address system and software updates and possible new threat that was found during screening.

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

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

(a) As part of initial training for new users;

(b) When required by information system changes; and

(c) [*FedRAMP Assignment: at least annually*] thereafter.

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

AT-2 What is the solution and how is it implemented?	
Part a	For the new users as part of their onboarding process will be subjected to a number of learning/training series that would require them to attend classes and take up quizzes pertaining to their role and department and some general security training norms of the organization. The latter includes the structure of the information flow to maintain data encapsulation, ethics of handling the data and the rights of data subjects, the former can delve into the specifics of the etiquettes followed by the department that works with the congress, practices with regards to safe maintenance of the chips by the bio team and so on.
Part b	Any changes within the information system has to be updated accordingly in the onboarding

AT-2 What is the solution and how is it implemented?	
	curriculum for all the effected entities with in the organization. A newsletter has to be published for all the existing users to know about the changes applied with in the system, this may also have to escalate to a knowledge transfer session based on the gravity of the change.
Part c	Updates to the onboarding series has to be made semi annually or any time a change arises within the information system, as per the newsletter distribution informing current users of the change, it has to happen once the changes have been well documented.

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

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

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

AT-2 (2) What is the solution and how is it implemented?
Upon the recognition of potentially dangerous indicators of insider threat, the security team has to investigate in and around the threatening party. Since the organization has to follow various security and privacy guidelines by HIPAA, GDPR and so on the security team has to take effective and immediate action in addressing a potential threat, if the threat is intentional, an arrest warrant can be issued upon the user and they have to submit themselves in the court of law. If the threat is unintentional, the user will have to go through probation and parallel supplemental training by an officer from a member of the IT Security Team.

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

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

(a) Before authorizing access to the information system or performing assigned duties;

(b) When required by information system changes; and

(c) [*FedRAMP Assignment: at least annually*] thereafter.

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

AT-3 What is the solution and how is it implemented?	
Part a	Company personnel are first given an initial training that gives an introduction about the importance of security in organisation. The content of the training is decided based on the roles. The security privileges that are present for each role are taken care of when training is given. Each role has different tasks to perform and based on that, training is tailored made in order to suit the specific role, the roles include - Chief Executive Officer, Chief of Risk Management, Senior Manager of Information Security,System administrator,Developer and Auditor as per our company policies.
Part b	The content of the training is subject to a update when there is such a situation that demands it. Situation that we anticipate are - privacy and security incidents resulting in data and accounts breach,findings from audit, changes in laws that govern IT security, changes in policies,directives,regulations,standards and guidelines. The Security Trainer regularly checks in with Security Enhancement Officer and Document Specialist to stay updated about the changes in Security regulations. They are tasked with simplifying the terms

AT-3 What is the solution and how is it implemented?	
	suitable to the intended audience for better understanding.
Part c	The training is undertaken every year. It will take place on the company premises. The training will comprise of general training and role-specific training. The general training session will have all the company personnel participating. Each of the company personnel at some level in executing their task are prone to encountering security threat, and hence the general training is intended to educate on this. The role-specific training will be scheduled the next to focus on individuals who are in those specific roles. Assessment takes place at the end of the training and personnels are issued certification.

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

The organization:

(a) Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

(b) Retains individual training records for [*FedRAMP Assignment: at least one year*].

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

AT-4 What is the solution and how is it implemented?	
Part a	Security Enhancement Officer have been working hard to maintain a safe and secure atmosphere by running awareness programs, campaigns, commercials, and sanitizing staff members towards maintaining healthy and secure environment. How do we assess the security culture is a legitimate concern. For this, a Security Enhancement Officer verifies and

AT-4 What is the solution and how is it implemented?	
	keeps track of every employee in the company like training are completed as per the policy and procedures implemented by the company. Every corporate employee is required to finish the provided security training within the allotted period. These trainings change depending on the position. The Security Enhancement Officer keeps accurate records for each employee. Every employee in the company should be aware of his or her duties and work to promote a culture of safety.
Part b	Security Enhancement Officer keeps tabs on the employee's activities and maintain a database that is kept as company records. The Security Enhancement Officer can retrieve the information from the company's records and present the one-year-old information if employee records are needed for the FedRAMP in the future.Organisations are to be flexible enough to adopt the ever-changing requirements so security trainings are conducted every year. and database is maintained as per year wise.

13.3. Audit and Accountability (AU)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(b) Reviews and updates the current:

(1) Audit and accountability policy [*FedRAMP Assignment: at every 3 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):	

AU-1	Control Summary Information
☐ Implemented ☐ Partially implemented ☐ Planned ☐ 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	

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

The organization:

(a) 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*];

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;

Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

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 Additional FedRAMP Requirements and Guidance:

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

AU-2	Control Summary Information
Responsible Role: Audit Manager	

AU-2	Control Summary Information
Parameter AU-2(a): Password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, third-party credential usage, account management events, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.	
Parameter AU-2(d): Access to confidential data, repeated failed attempts to login, data deletions, data changes, and data transfer are audited continually.	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-2 What is the solution and how is it implemented?	
Part a	The information system is capable of auditing the audit events including password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage, account management events, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. The information system constantly creates logs for every activity from each of the accounts including individual and groups and stores them in a secured NoSQL databases with time stamps. Reports are generated from these data and are shared with the security management department.
Part b	The audit results are reports are shared with the security management department for them to take actions when there is any suspicious activity in the information system that includes access to any confidential data from unauthenticated personnel or repeated unsuccessful login attempts from an account. The security management department may work with the audit management to point out the auditable events and what cases may lead to security threat and breaches that they should be aware of. This will help the security management to do a root cause analysis when there is a case of possible threat and how to ensure its prevention.
Part c	The audit management and the security management agrees upon the reasons on why auditable events are appropriate for finding the root cause of the security threat or breach that may occur and what consequences can arise from these security threats. They share a

AU-2 What is the solution and how is it implemented?	
	documentation between them that specifies some rules and rationale on how and why some audit events are necessary. The security management may also suggest the audit management to grab more information in their logs that may be crucial at the time of investigation, how to interpret the information and provide them with the detailed report of it.
Part d	The events that are audited includes password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage, unauthorized access to confidential data, account management events, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Of these audit events, the access to the privileged resources like personal and biological information of the criminals, data deletions, data changes, data transfer and repeated failed logins are continuously audited by the audit management whether they are being accessed by the authorized personnel. The other audit events that includes password change, account management events are audited daily at 8 pm.

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

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/AO.

AU-2 (3)	Control Summary Information
Responsible Role: Audit Manager and Security Manager	
Parameter AU-2(3): Annually or as per requirement basis when changes in the threat environment are communicated to the service provider by the JAB/AO or whenever a potential threat is encountered	
Implementation Status (check all that apply): ✅Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)	

AU-2 (3)	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-2 (3) What is the solution and how is it implemented?
The events that needs to be audited and how they are going to be audited are finalized upon by security management and the audit management. At the beginning month of each year the security management and the audit management conduct a meeting to discuss the changes in the events or changes in the process of auditing the events. Changes may be made as per requirement basis when changes in the threat environment are communicated to the service provider by the JAB/AO or whenever a potential threat is encountered. In these cases the 2 departments conduct urgent meeting to agree upon some new audit events that they have missed or were not audited appropriately and add them to the list of audit events.

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

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

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

AU-3 What is the solution and how is it implemented?
The audit events include password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage, unauthorized access to confidential data, etc. The information system generates logs for all these audit events and stores them in NoSQL databases, from which reports can be generated by accessing these databases. The contents of the logs include the name of the username of the accounts (individual and groups), timestamp of access, the configuration updates, the data and files read and written, the data and file transfers, total active time, number of unsuccessful attempts to log in, the physical location of login, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes, state of the system after these changes, etc.

AU-3 (1) Control Enhancement (M)

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

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

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

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

AU-3 (1)	**Control Summary Information**
Responsible Role: Audit Manager	
Parameter AU-3(1): Byte count and time taken during a transaction in the information system	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-3 (1) What is the solution and how is it implemented?
The information system will be logging any communication between a client and a server, where clients can be an individual or a group, and between different accounts in terms of number of bytes transferred, the time taken to transfer data, the timestamp of the data transfer, the device used for the transfer, and the data sources and users involved in these transactions. These logs will be beneficial in investigation if there is a case of confidential information leak outside the system.

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

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

AU-4	Control Summary Information
Responsible Role: Internal Auditor	
Parameter AU-4: 100 GB storage	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-4 What is the solution and how is it implemented?
The organisation decides on the amount of storage requirement needed based on the type of audits that is performed and the requirements needed to perform the audit. The limit described is specific to company's needs such that we do not run out of storage limit and to avoid potential loss. The company is audited internally,externally by parent Government agency,compliance audits and information system audits. The input from relevant departments of the Organization is needed to undertake each of the different audit types. The requirements vary depending on planning,field work and report.

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

The information system:

(a) Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and

(b) Takes the following additional actions: [*FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)*].

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

AU-5 What is the solution and how is it implemented?	
Part a	The System Manager of the company is informed about audit processing failure. The logs occurring due to various activity in the company has to be stored and it is managed by System manager who is aware of status of the system and software. When there is a failure to register all the processing the System Manager is informed about the failure. There can be various possibilities for the failure to occur like software or hardware errors,network errors,failure to capture audits, or exceeding the audit storage limit.
Part b	On occurrence of audit processing failure oldest record is overwritten. Logs are registered in the system to keep track of events occurring, troubleshooting ,optimisation and maintenance. Failure can result in events being lost and unable to maintain track. The oldest log files when written onto disk is no more needed and hence the maintained log files are removed so that it creates space for the fresh logs. The old log files when has to be revisited can be retrieved from data recovery software managed by software manager of the company

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

The organization:

(a) Reviews and analyzes information system audit records [*FedRAMP Assignment: at least weekly*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

(b) Reports findings to [*Assignment: organization-defined personnel or roles*].

AU-6 Additional FedRAMP Requirements and Guidance:

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

AU-6	Control Summary Information
Responsible Role: Audit Manager	
Parameter AU-6(a)-1: Monitor and analyse the weekly Audit Information	
Parameter AU-6(a)-2: Look for potential Threat.	
Parameter AU-6(b): Any unusual activity will be reported to Security Group	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-6 What is the solution and how is it implemented?	
Part a	Every employee's action is tracked by the organization, and a report is produced. This report includes statistics on logins, remote access to databases or servers, network configuration changes, and the number of devices each employee uses to log in to the company server. Weekly report collection and analysis are done by the audit manager, who then creates a final report. The security team receives this last reporting.
Part b	The Audit Manager will prepare a report on the employee after carefully investigating and submitting

AU-6 What is the solution and how is it implemented?	
	the report to the higher security management if any suspicious activity is discovered during the analysis. The team will gather the employee to discuss the action and give him the chance to defend himself. If the accuser is unable to prove the claim, he or she will be held legally liable in accordance with corporate policy.

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

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

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

AU-6 (1) What is the solution and how is it implemented?
It's critical to maintain the pace in order to benefit from emerging technical advancements and boost production. Until recently, it was difficult to maintain track of organizational records. There was a ton of paperwork, but as time goes on, the procedure also does. But now that this problem has been solved, everything is automated. Software that runs in the background and has corporate policies built in. It will mark any improper activity if it is found. Automation reduces mistake while speeding up processes.

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

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

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

AU-6 (3) What is the solution and how is it implemented?
After the reports are prepared, the analyst runs a program that contains the data from many organizations. It evaluates the specifics and determines whether a corporation is falling behind on certain security measures. This analysis will provide information on risk management, including specifics on how to strengthen security, address loopholes, and conduct awareness campaigns, commercials, and sanitization training for staff in order to maintain a safe and secure environment.

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

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

(a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

(b) Does not alter the original content or time ordering of audit records.

AU-7	Control Summary Information
Responsible Role: Security Audit Officer	
Implementation Status (check all that apply): ☐ Implemented ✅ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

AU-7	Control Summary Information
☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-7 What is the solution and how is it implemented?	
Part a	The Security Audit Officer, among their other duties, goes through the audit logs and information to conduct audit reduction. They essentially abridge the data, statistics, security incidents in a summary format. The officer and their entourage should conduct a thorough review and proof reading making sure everything has been conveyed correctly as intended.
Part b	Generation of customizable audit reports which can be worked upon for further refinement is the planned proposition. Data science and Hadoop techniques can be used to detect anomalies within the logs to get things started with report refinement.

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

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

AU-7 (1)	Control Summary Information
Responsible Role: Security Audit Officer	
Parameter AU-7(1): information flow standards, security protocols among others	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ✅ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-7 (1) What is the solution and how is it implemented?
The audit records are made very processible and accessible and design for seamless access to the organization defined audit fields like access control protocols, permissions, security protocols, firewalls and private networks, their statistics, logs and standards. These records will clearly depict if the variable parameters are meeting the required standards of the audit. The security Audit officer would aim for at most accuracy and transparency.

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

The information system:

(a) Uses internal system clocks to generate time stamps for audit records; and

(b) Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: one second 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The information system:

(a) Compares the internal information system clocks with [*FedRAMP Assignment: authoritative time source:* [*http://tf.nist.gov/tf-cgi/servers.cgi*] *[at least hourly]*]; and

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

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

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

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

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

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

AU-8 (1)	Control Summary Information
Responsible Role:	
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)	

AU-8 (1)	Control Summary Information
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

AU-9 (4)	Control 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)	

AU-9 (4)	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

AU-11 Audit Record Retention (M)

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

AU-11 Additional FedRAMP Requirements and Guidance:

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

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

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

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

The information system:

(a) 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*];

(b) Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and

(c) Generates audit records for the events defined in AU-2 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

13.4. Security Assessment and Authorization (CA)

CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

(a) Reviews and updates the current:

(1) Security assessment and authorization policy [*FedRAMP Assignment: at least every three (3) 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	

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

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

The organization:

(a) 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;

(b) 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;

(c) Produces a security assessment report that documents the results of the assessment; and

(d) Provides the results of the security control assessment to [*FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)*].

CA-2 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Annual Assessment Guidance https://www.fedramp.gov/documents/

CA-2	Control Summary Information
Responsible Role:	
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)	

CA-2	Control Summary Information
☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization,	

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

CA-2 (1) Control Enhancement (L) (M) (H)

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

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

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

CA-2 (1)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

CA-2 (2) Control Enhancement (M) (H)

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

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

Requirement: To include *'announced', 'vulnerability scanning' to occur at least annually*.

CA-2 (2)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

CA-2 (3) Control Enhancement (M) (H)

The organization accepts the results of an assessment of [*FedRAMP Assignment: organization-defined information system*] performed by [*FedRAMP Assignment: any FedRAMP Accredited 3PAO*] when the assessment meets [*FedRAMP Assignment: the conditions of the* JAB/AO *in the FedRAMP Repository*].

CA-2 (3)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

CA-3 System Interconnections (L) (M) (H)

The organization:

(a) Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

(a) Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

(b) Reviews and updates Interconnection Security Agreements [*FedRAMP Assignment: at least annually and on input from FedRAMP*].

Table 13-3. CA-3 Authorized Connections

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

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

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

CA-3 (3) Control Enhancement (M) (H)

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:

Guidance: Refer to Appendix H – Cloud Considerations of the TIC Reference Architecture document. Link: https://www.dhs.gov/publication/tic-reference-architecture-22

CA-3 (3)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

CA-3 (5) Control Enhancement (M)

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 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

(a) 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: Plan of Action & Milestones (POA&M) must be provided at least monthly.

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Plan of Action and Milestones (POA&M) Template Completion Guide
https://www.FedRAMP.gov/documents/

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

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

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

The organization:

(a) Assigns a senior-level executive or manager as the authorizing official for the information system;

(a) Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

(b) Updates the security authorization [*FedRAMP Assignment: in accordance with OMB A-130 requirements 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 (SP 800-37). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

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

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

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

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

(a) Establishment of [*Assignment: organization-defined metrics*] to be monitored;

(a) Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;

(b) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

(c) Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

(d) Correlation and analysis of security-related information generated by assessments and monitoring;

(e) Response actions to address results of the analysis of security-related information; and

(f) 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:

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

Guidance: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide

https://www.fedramp.gov/documents/

CA-7	Control Summary Information
Responsible Role:	
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)	

CA-7	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

CA-7 (1) Control Enhancement (M) (H)

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 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

CA-8 Penetration Testing (M) (H)

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

CA-8 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Penetration Test Guidance

https://www.fedramp.gov/documents/

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

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

CA-8 (1) Control Enhancement (M) (H)

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

CA-8 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

CA-8 (I)	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and

(a) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

13.5. Configuration Management (CM)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]:*

(1) A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(b) Reviews and updates the current:

(1) Configuration management policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Configuration management procedures [*FedRAMP Assignment: at least annually*].

CM-1	Control 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)	

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

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

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

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

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

CM-2 (1) Control Enhancement (M)

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

(a) [*FedRAMP Assignment: at least annually*];

(a) When required due to [*FedRAMP Assignment: to include when directed by the JAB*]; and

(b) As an integral part of information system component installations and upgrades.

CM-2 (1)	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

CM-2 (2)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

CM-2 (2)	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

CM-2 (3) Control Enhancement (M)

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

CM-2 (3)	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(a) Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

CM-2 (7)	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Determines the types of changes to the information system that are configuration-controlled;

(a) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

(b) Documents configuration change decisions associated with the information system;

(c) Implements approved configuration-controlled changes to the information system;

(d) Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

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

Guidance: In accordance with record retention policies and procedures.

(e) Audits and reviews activities associated with configuration-controlled changes to the information system; and

(f) Coordinates and provides oversight for configuration change control activities through [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

CM-3 Additional FedRAMP Requirements and Guidance:

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

CM-3	Control Summary Information
Responsible Role:	
Parameter CM-3(e):	
Parameter CM-3(g)-1:	
Parameter CM-3(g)-2:	
Parameter CM-3(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)	

CM-3	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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

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

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

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

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

CM-5 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

CM-5 (1)	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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:

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

CM-5 (3)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Limits privileges to change information system components and system-related information within a production or operational environment; and

(b) Reviews and reevaluates privileges [*FedRAMP Assignment: at least quarterly*].

CM-5 (5)	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Establishes and documents configuration settings for information technology products employed within the information system using [*FedRAMP Assignment: see CM-6(a)*

Additional FedRAMP Requirements and Guidance] that reflect the most restrictive mode consistent with operational requirements;

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

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

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

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

(a) Implements the configuration settings;

(b) 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

(c) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

CM-6	Control Summary Information
Responsible Role:	
Parameter CM-6(a)-1:	
Parameter CM-6(a)-2:	
Parameter CM-6(c)-1:	
Parameter CM-6(c)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

CM-6 (1)	**Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Configures the information system to provide only essential capabilities; and

(b) Prohibits or restricts the use of the following functions, ports, protocols, and/or services [*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. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

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

Partially derived from AC-17 (8).

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

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

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

The organization:

(a) Reviews the information system [*FedRAMP Assignment: at least Monthly*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

(b) Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].

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

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

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

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

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

CM-7 (5) Control Enhancement (M)

The organization:

(a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];

(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

(c) Reviews and updates the list of authorized software programs [*FedRAMP Assignment: at least annually or when there is a change*].

CM-7 (5)	Control Summary Information
Responsible Role:	
Parameter CM-7(5)(a):	
Parameter CM-7(5)(c):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

CM-7 (5)	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Develops and documents an inventory of information system components that:

(1) Accurately reflects the current information system;
(2) Includes all components within the authorization boundary of the information system;
(3) Is at the level of granularity deemed necessary for tracking and reporting; and
(4) Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

(b) Reviews and updates the information system component inventory [*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):	

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

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

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

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

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

Delete this and all other instructions from your final version of this document.

CM-8 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)	

CM-8 (1)	Control Summary Information
☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) 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

(b) Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables network access by such components; isolates the components; notifies* [*Assignment: organization-defined personnel or roles*]].

CM-8 (3)	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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

(a) Addresses roles, responsibilities, and configuration management processes and procedures;

(b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

(c) Defines the configuration items for the information system and places the configuration items under configuration management; and

(d) Protects the configuration management plan 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Uses software and associated documentation in accordance with contract agreements and copyright laws;

(b) Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

(c) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

CM-10 (1)	Control Summary Information
Responsible Role:	
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)	

CM-10 (1)	Control Summary Information
☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

CM-10 (1) What is the solution and how is it implemented?

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

The organization:

(a) Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;

(b) Enforces software installation policies through [*Assignment: organization-defined methods*]; and

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

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

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

13.6. Contingency Planning (CP)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(b) Reviews and updates the current:

(1) Contingency planning policy [*FedRAMP Assignment: at least every three (3) years*].; and

(2) Contingency planning procedures [*FedRAMP Assignment: at least annually*].

CP-1	Control Summary Information
Responsible Role: Contingency Planning Manager	
Parameter CP-1(a): Contingency Planning Department	
Parameter CP-1(b)(1): Every 3 years	
Parameter CP-1(b)(2): Annually	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific)	

CP-1 What is the solution and how is it implemented?	
Part a	The Contingency Planning Manager develops documents related the control that are used to address the policy and procedures that are going to affect the security control over the system and the organization overall to reflect the current federal laws, standards, regulations, etc. The policies and procedures are based on forthcoming security control changes and risks and are helpful in risk management. These policies and procedures are in general for the entire organization and also specific to roles, purpose, scope, compliance and responsibilities for different account types in the organization to safeguard against any anticipated threat and disruption. These documentations are developed and distributed to every employee in the organization with the policies and procedures to maintain the security compliance and controls at organization and system specific level up to date and prepared for anticipated future incidents. These plans will include backing up databases, servers, how to close the systems that has been affected by threat without affecting the others, backing up virtual machines, etc.
Part b	The current contingency planning procedure is updated every 3 years unless there is a security threat that has been encountered in the system. In this case, the policies are changed with immediate effect after analyzing the security threat and what loop holds in the policies resulted in the threat. The contingency planning manager conducts a meeting with the higher officials of the organization to discuss the update in policies. The contingency procedures are updated every year due to newer and advanced security technologies come into the market more often, and the organization will update the procedures on the basis of new security technologies in the market. Like policies, if there is a security threat in the system, the procedures are tested and analyzed to check if any loose ends in the procedures may have resulted in the threat. In that case, the procedures are updated with implementation fixes with immediate effect.

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

The organization:

(a) 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*];

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

(d) Coordinates contingency planning activities with incident handling activities;

(e) Reviews the contingency plan for the information system [*FedRAMP Assignment: at least annually*];

(f) 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;

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

(h) Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

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

CP-2	Control Summary Information
Responsible Role: Manager	
Parameter CP-2(a)(6): Chief Information Officer	
Parameter CP-2(b): Information System Security Officer	
Parameter CP-2(d): Annually	
Parameter CP-2(f): System Engineer	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

CP-2 What is the solution and how is it implemented?	
Part a	Contingency plan is developed for the information system by the organisation. The plan takes into consideration the essential missions of the company which is monitoring of the parolees who are out of the prison. All the functionalities of the information system that goes into monitoring are taken care of while creating contingency plan so that the essential mission is not affected by any disruption and is kept running according to the contingency plan that recommends the restorative actions

CP-2 What is the solution and how is it implemented?	
Part b	The organisation distributes copies of contingency plans to the essential department that is involved in managing the activities of the company when there is system disruption in order to bring back the system and to keep-it up and running. The contingency plan contains alternate operation modes when the system is under attack along with necessary steps in order to execute the plan. By having the copies of the plan with the necessary department, on occurrence of security incident, the respondible department can quickly launch restorative measures.
Part c	The organisation coordinates contingency planning activities with incident handling activities. Having a contingency plan for the company necessitates series of course of actions that has to be executed in order to achieve continuity of operations of businesses. The contingency plan is thus executed in coordination with the incident handling team that has necessary technical skills to execute the contingency plans.
Part d	The company reviews contingency plans annually. Reviewing the contingency plans is essential to keep up with the changing laws and regulations and change in the system due to addition of new features that require new skillset and new course of actions to execute it. The review helps in suggesting changes to the existing contingency plan such that it considers the update in the system.
Part e	The company updates the contingency plan to address the changes in the organisation. The organisation can under go changes in management, that shifts the responsibility to the new personnel that take up the position in the management, who has to be included in the contingency plan. Technical changes to the information system is updated in the new contingency plan. Initial problems that were encountered in the planning is resolved to update in the new contingency plan.
Part f	The company communicates contingency plan changes to concerned department. The company after reviewing the existing contingency plan and making updates to it as necessary commuciates the changes made to the concerned department to inform them about the changes in the contingency plan and the possible actions to be performed in order to ensure the continuity of the system when it encounters a disruption.
Part g	The organisation protects the contingency plan from unauthorized disclosure and modification. The contingency plan is the result of inputs received from Manager, Chief Information Officer, The Information Security Officer and the System Architects. Nobody out of this committee has the authorization to edit the contingency plan as they do not have sufficient knowledge or background in handling the incident when the system is under attack. The edit rights are only given to the personnel involved in creating the contingency plan.

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

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

CP-2 (1)	Control Summary Information
Responsible Role: Senior Agency Information Security Officer	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented	

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

CP-2 (1) What is the solution and how is it implemented?
The contingency plan involves steps to be taken in-order to ensure continuity in the system on occurrence of system failure. All the departments in the company involved in the tasks that have to be performed to ensure the system continuity have to be involved executing the tasks. The plans include Business continuity plans,Disaster recovery plans,continuity of operations,crisis communication plans,critical communication plans,Cyber Incident plans,Inside threat implementation and occupant emergency plans.

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

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

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

CP-2 (2) What is the solution and how is it implemented?
The capacity planning is made in-order to prepare for the critical state when system is under attack. An assessment of the available resources in the company and analysis of how the resources can de-grade under the system attack is conducted. The threats that affect the system can result in available systems for processing,telecommunications, and support services that are critical to business and mission functions, performing below par the expected. Capacity planning helps in making the systems available to perform operations continuously.

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

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 Summary Information
Responsible Role: Chief Information Officer	
Parameter CP-2(3): 24 hours	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

CP-2 (3) What is the solution and how is it implemented?
The essential missions and business functions resume within 24 hrs of contingency plan being activated. The period decided considers the highest level of system attack possible to the information system. Other lower level risks and attacks possible to the system can halt the essential missions and business functions for lesser time than 24 hrs bringing the system back to running in less time. The department concerned in contingency planning execute the necessary tasks to bring the system to work and function.

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

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

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

CP-2 (8) What is the solution and how is it implemented?
The organisation identifies critical informtion system assets that are essential in operation of the organisation. Identifying the critical assets involve finding additional resources and measures to ensure the system can run during the activation of contingency planning activities. Identification of critical assets helps in prioritizing the system resources during the contingency plan execution. The system resources includes technical and operations aspects. Technical aspects includes information system related services,components,products and mechanism. Operational aspects involve procedures and personnel. Organisation has program protection plans that help in identifying critical assets.

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

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

(a) Within [*FedRAMP Assignment: ten (10) days*] of assuming a contingency role or responsibility;

(i) When required by information system changes; and

(j) [*FedRAMP Assignment: at least annually*] thereafter.

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

CP-3 What is the solution and how is it implemented?
The company provides contingency training to secure the information systems. Each employee participating in this training must finish it in the allowed time. According to the designation, training levels are assigned. While upper management will receive advanced training, common staff will only receive basic training. To lessen the security concern, this training will cover every job and duty within the organization. Employees will get training modules, including instruction on general rules, security procedures, codes of behavior, which they must do and submit within the allocated 10-day time frame.The program will provide up-to-date knowledge on current security issues. It takes place each year. There are company policies that must be adhered to when completing the training, such as using the company network and only opening the training on the laptop that was provided by the company.

CP-4 Contingency Plan Testing (M)

The organization:

(a) Tests the contingency plan for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: functional exercises*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

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

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

(k) Reviews the contingency plan test results; and

(l) Initiates corrective actions, if needed.

CP-4	Control Summary Information
Responsible Role: Contingency Tester	
Parameter CP-4(a)-1: Annually	
Parameter CP-4(a)-2: Risk analysis and security system monitoring	
Implementation Status (check all that apply): ☐ Implemented ✅ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

CP-4 What is the solution and how is it implemented?	
Part a	The contingency tester and System security specialist would schedule sessions to work together on the contingency plan for the information system. This includes unit testing, to ensure all individual elements work well as a stand alone unit and process testing where they check for anomalies and make sure the contingency plan would work and all the pieces work in tandem to each other.
Part b	The plan is reviewed and discussed among the managers, Contingency tester, Security System Specialist and audit advisor. Changes are proposed where ever necessary and is approved after everyone's suggestions are addressed.
Part c	Corrective actions are directed by the committee over seeing the reviews of the contingency plans. Suggestions are made and the contingency tester and security specialist can work on solutionsto further police the contingency plan and eventually its execution.

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

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

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

CP-4 (1) What is the solution and how is it implemented?
The ocntungency Tester plans and organization a group review system where managers, representatives from the information system security team, the information security specialist, audit reviewer among others gather in two phases. In the first phase the go through the contingency and mitigation plans, make notes, and discuss it. The Contingency planner and the Security Specialist then test the comments and the behavioral patterns on the contingency plans given the parameters and scencarios proposed in the phase 1. Finally in phase 2, the cohort is presented by the findings of the testing and are then requested to review and approve if their conditions are met.

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

The organization:

(a) Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

(a) 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	

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

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

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

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

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

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

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

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

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

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

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

The organization:

(a) Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*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.

(m) 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

(n) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

CP-7 (1) Additional FedRAMP Requirements and Guidance

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

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

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

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

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

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

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

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

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

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

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

CP-8 Telecommunications Services (M) (H)

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 recovery time objectives and 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 (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

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

(a) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply):	

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

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

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

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

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

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

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

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

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

(a) 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).

(o) 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).

(p) 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).

(q) Protects the confidentiality, integrity, and availability of backup information at storage locations.

CP-9	Control Summary Information
Responsible Role:	
Parameter CP-9(a):	
Parameter CP-9(b):	
Parameter CP-9(c):	

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

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

CP-9 (1) Control Enhancement (M)

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

CP-9 (1)	Control 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)	

CP-9 (1)	Control Summary Information
☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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

CP-10 (2)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

CP-10 (2)	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

13.7. Identification and Authentication (IA)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(b) Reviews and updates the current:

(1) Identification and authentication policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Identification and authentication procedures [*FedRAMP Assignment: at least annually*].

IA-1	Control Summary Information
Responsible Role:	
Parameter IA-1(a):	
Parameter IA-1(a):	
Parameter IA-1(b)(1):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

IA-1	Control Summary Information
☐ 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	

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

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

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

IA-2 What is the solution and how is it implemented?
The accounts manager accepts the request of account creation of organizational users requests. The accounts manager reviews the requests along with the access types which might be local or network access. These accounts are provided with credentials and rule documentation on how to access their accounts through either local or network access. The accounts manager reviews the request and verifies whether the authentication requirements are complying with the requirements of homeland security. These accounts like other accounts require multifactor authentication where first the user would be asked to provide their password, then they would be asked for a unique token in their personal device for network access. The number of factoring varies for privileged and non privileged accounts. If the user enters wrong password for 3 times, the account will be blocked and same applies to entering wrong token for 3 times. For local access, the user should be on premise and should login through some designated machines assigned to them using different credentials. Some of these accounts are given VPN access to the local network based on the severity of their work and it also require multifactor authentication. All these accesses will be monitored.

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

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

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

IA-2 (1) What is the solution and how is it implemented?
The accounts manager approves the request of account creation of privileges accounts with a 3 factoring authentication as these accounts have access to more confidential resources than the non privileged ones. For the network access, the first authentication would be a password, then it would require them to provide a valid token that would be generated on their personal devices. The third authentication would be a biometric where they would be asked scan their fingerprint in a designated hardware device that will be connected to the network. The accesses will be monitored real time.

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

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

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

IA-2 (2) What is the solution and how is it implemented?
The accounts manager approves the request of account creation of non privileges accounts with a 2 factoring authentication as these accounts do not have access to more confidential resources. For the network access, the first authentication would be a password, then it would require them to provide a valid token that would be generated on their personal devices. The accesses will be monitored real time.

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

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

IA-2 (3)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented	

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

IA-2 (3) What is the solution and how is it implemented?
For local access for privileged accounts, it is recommended to be on premise, but depending on the varsity of work, users would require a different credential for VPN access and same 3 factoring authentication. When on premise, there are only allowed to access their accounts from their designated systems using 2 factor authentication excluding the biometric.

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

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

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

IA-2 (5) What is the solution and how is it implemented?
To dodge the risks from group authenticator, the information security officer and their team can supplement as a supplemental individual authenticator. The information security office and his team would have more security checks to successfully authenticate and individual user. This implementation can be used to ensure save authentication in scenarios where users want to access data that is restricted to them under normal circumstances but have privileges to access the same.

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

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

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

IA-2 (8) What is the solution and how is it implemented?
With a human authenticator in play to authorize special privilege accesses for users can help in avoiding authentication replay. And on the other hand, while using external applications for facilitating multi factor authentication, to protect against the tapping and capturing the transfer of authentication data and uniquely identifiable information everything is encrypted by the ever changing and updating organization's protocol to ensure safe transfer over public networks before giving network access to privileged accounts.

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

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*FedRAMP Assignment: FIPS 140-2, NIAP* Certification, or NSA approval*].

*National Information Assurance Partnership (NIAP)

Additional FedRAMP Requirements and Guidance:

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

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

IA-2 (11) What is the solution and how is it implemented?
The IT of the organization will be using an Authentication application for remote access to privileges and non-privilaged accounts to facilitate two factor authentication. The organization is planning to use Microsoft's authenticator to allow legitimate users to authenticate themselves using a secondary device. Their secondary device is organization issued mobile device with restrictive environment where the users can only have official contacts, can not install any third party applications and has to be in the possession of the user at all times.

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

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

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

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

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

IA-2 (12) What is the solution and how is it implemented?
The information systems supports a Logical access control sub-system to maintain the personal identity verification mechanism for establishing intended access control and information flow. This system is designed to handle any special scenario that might contradict the company’s logical access control and make accommodations accordingly as long as the personal identity verification system still adhere to FIPS Publication 201 and supporting guidance documents and ensure a company wide secure use of PIV credentials.

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

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: Security Analyst	
Parameter IA-3-1: MAC address and Username and Password	
Parameter IA-3-2: Local, Remote connection	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

IA-3	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☑ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IA-3 What is the solution and how is it implemented?
Employees must install security software for a secure network connection to the corporate website. The business has a virtual private network of its own. The IT department will install this security software on the person's device, enabling them to connect to the corporate network. The employees can log into the server after the software has been installed using their own authentication user ID and password, which will record the MAC address of the device and keep a database for future authentication. These details are gathered so that security analysts can identify, authenticate, and keep an eye on device access if any employees connect to the company network remotely rather than locally. To access company records remotely, an employee must be connected to a VPN. After logging in to the server with their individual authentication user ID and password, the software will conduct a background check to find and validate the MAC address connected to the userID. Access will be denied and a report as to an unauthorized login will be generated if authentication fails. Further, the Security Analyst will confirm the same with the Employee.

IA-4 Identifier Management (L) (M)

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

(a) Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

(c) Selecting an identifier that identifies an individual, group, role, or device;

(d) Assigning the identifier to the intended individual, group, role, or device;

(e) Preventing reuse of identifiers for [*FedRAMP Assignment: at least two (2) years*]; and

(f) Disabling the identifier after [*FedRAMP Assignment: ninety days for user identifiers (see additional requirements and guidance)*]

IA-4e Additional FedRAMP Requirements and Guidance:

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

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

IA-4	Control Summary Information
Responsible Role: Information Identity Manager	
Parameter IA-4(a): Information Security Officer	
Parameter IA-4(d): 2 years	
Parameter IA-4(e): 90 days	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IA-4 What is the solution and how is it implemented?	
Part a	An authorization has to be issued from Information Security Officer to issue identitiers to all the users using the system. The Homeland Security Department has different levels of working staff, who use the system to monitor the parolees. Based on the rank of the staff identifiers are issued that takes in their name, employee ID, number of years of service,retirement year,level of privileges available to the employee,their higher reporting officer.
Part b	An identifier includes name, employee ID, number of years of service,retirement year,level of privileges available to the employee,their higher reporting officer, as the general information for all employee staff. The staff that has higher level of privilege will be an additional information that comprises in the identifier. For temporary access of restricted services, member staff with recognised and verified background information receive limited access to privilege services that will be included in the identifier.
Part c	An identifier is assigned to the staff after they have been onboarded to serve Homeland Security. They initially would be having basic identifier provided to them. As the requirement arises to include more staff into monitoring and tracking of parolees from our system staff are issued updated identifiers that include all the necessary access for them to operate,monitor and share information collected from the system in their department.
Part d	An identifier that is issued to a staff member has to be restricted to being unique. Everytime a new

IA-4 What is the solution and how is it implemented?	
	identifier has to be created to a new user. Our system prevents using same identifiers used by different people to access the same system. Our system keeps track of incidences of reusing of the same identifier everytime. If the number crosses the number established by the Information Security Officer, the identifier will be blocked until verification proves that the incidence was unharming.
Part e	The identifiers that are not used for 90 days to actively log in to system and use it's services will be disabled without warning notification. The user is aware of the defined period of inactivity so that it doesn't come in the way of their duty. The time period is well defined to consider the activities of the staff members. Every staff member works in rotation to use the system and it should be actively used. If the reasons to not use the system include non-security issues like personal and medical conditions of the staff, the identifier is reactivated on case by case basis.

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

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

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

IA-4 (4) What is the solution and how is it implemented?
The identifiers identifies the users of the systems as Organisational Staff Members who use the system regularly. The user should be U.S National Citizen, recruited by Homeland Security to serve the Government. Our system relies on the background verification information provided by the Homeland Security to assign the identifiers to the users. The system manages the accounts of the user by logging their activities of usage, reports suspicious activities, disables the identifier when the inactivity period reached the period set by the system.

IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

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

(g) Establishing initial authenticator content for authenticators defined by the organization;

(h) Ensuring that authenticators have sufficient strength of mechanism for their intended use;

(i) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

(j) Changing default content of authenticators prior to information system installation;

(k) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

(l) Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*].

(m) Protecting authenticator content from unauthorized disclosure and modification;

(n) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

(o) Changing authenticators for group/role accounts when membership to those accounts changes.

IA-5 Additional FedRAMP Requirements and Guidance:

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

IA-5	Control Summary Information
Responsible Role:	
Parameter IA-5(g):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

IA-5	Control Summary Information
☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(p) Enforces at least the following number of changed characters when new passwords are created: [*FedRAMP Assignment: at least one (1)*];

(q) Stores and transmits only cryptographically-protected passwords;

(r) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization- defined numbers for lifetime minimum, lifetime maximum*];

(s) Prohibits password reuse for [*FedRAMP Assignment: twenty-four (24)*] generations; and

(t) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

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

Guidance: If password policies are compliant with NIST SP 800-63B Memorized Secret

(Section 5.1.1) Guidance, the control may be considered compliant.

IA-5 (1)	Control Summary Information
Responsible Role:	
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 ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The information system, for PKI-based authentication:

(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

(b) Enforces authorized access to the corresponding private key;

(c) Maps the authenticated identity to the account of the individual or group; and

(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

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

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

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

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 Summary Information
Responsible Role:	
Parameter IA-5(3)-1:	
Parameter IA-5(3)-2:	
Parameter IA-5(3)-3:	

IA-5 (3)	Control Summary Information
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

IA-5 (4) Control Enhancement (M)

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 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	

IA-5 (4)	Control Summary Information
☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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

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

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

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

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

IA-5 (11)	Control 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):	

IA-5 (11)	Control Summary Information
☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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	

IA-8	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

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

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

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

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

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

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

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

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

IA-8 (3)	Control Summary Information
Responsible Role:	
Parameter IA-8(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	

IA-8 (3)	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The information system conforms to FICAM-issued profiles.

IA-8 (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) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

13.8. Incident Response (IR)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

(u) Reviews and updates the current:

(1) Incident response policy [*FedRAMP Assignment: at least every three (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	

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

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

(a) Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;

(v) When required by information system changes; and

(w) [*FedRAMP Assignment: at least annually*] thereafter.

IR-2	Control Summary Information
Responsible Role: Incident Response training Manager	
Parameter IR-2(a): 30 working days	
Parameter IR-2(c): Anually	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IR-2 What is the solution and how is it implemented?	
Part a	The incident response training is provided to all account types within the organization. These training is specific the account type and also involves training of responses to general security incidents. The training is provided to resolve the effect of the incident within 30 days of the occurrence. The users need to report the incident within 1 day of the detection to give the administration and the responders sufficient time to analyse the threat and take necessary measure for restoration and system recovery.
Part b	The training to the incident responses may get altered due to changes in the information system. Whenever there is a software update, or implementation of new technology solutions like update of event log monitoring software, firewalls, antiviruses, the responsible roles must be made up to date with the procedure of analysis of an incident and how to detect threats in the updated technologies and also make them aware of new incidents that might occur with these new implementations.
Part c	The trainings are held annually for each of the account type keeping in mind their responsibilities and

IR-2 What is the solution and how is it implemented?	
	access over the resources and data. The end users are given sufficient training to detect an suspicious incident in there accounts and report it with sufficient details to help the administration and responders analyse the entire incident and takes necessary steps to mitigate the effect of the security threats and fix bugs, implementation of the code and technology used in the system. The administrators are provided with training to handle the incidents, and responders are trained to fix the issue and make restorations to the affected part of the system within a limited time frame.

IR-3 Incident Response Testing (M)

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.

IR-3 Additional FedRAMP Requirements and Guidance:

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

IR-3	Control Summary Information
Responsible Role: Incident Manager	
Parameter IR-3-1: Annually	
Parameter IR-3-2: Test plans are approved and accepted by the JAB/AO prior to the test commencing.	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IR-3 What is the solution and how is it implemented?
To check for any weaknesses or flaws inside the organization, the company will conduct incident response testing. The organization will test how the employees are responding to the situation in a simulated incident scenario. There will be a check list for problem-solving. this test will be approved by JAB authorisation. The effectiveness of the organizational activities will be evaluated through this incident response testing. This testing will be carried out annually, and if the management is changed, the test will be carried out following the change. After identifying risks, we will analyze vast amounts of security telemetry in the areas where adversaries operate using advanced analytics.

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

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

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

IR-3 (2) What is the solution and how is it implemented?
The organization will keep track of test results and analyze them. After reviewing the report, the administration and emergency personnel can analyze the entire occurrence and take the required action to reduce the impact of security threats and address faults in the system's code and technology. With organizational components in charge of associated plans, the organization manages incident response testing. Business continuity plans,, disaster recovery plans, crisis communications plans, critical infrastructure plans are a few examples of organizational plans connected to incident response testing.

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

The organization:

(a) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

(b) Coordinates incident handling activities with contingency planning activities; and

(c) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional FedRAMP Requirements and Guidance:

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

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

IR-4 What is the solution and how is it implemented?	
Part a	All the security team personnel have trained and made aware about the incident handeling policies, registered/ historic incidents. The process starts with the Incident manager genearting an analysis report on the incident, then the team discussing mitigation and containment procedures among themselves, stake holders, all the effected parties and all other appropriate entities with respect to the weight of the incident. After gaining in depth analysis on the incident, the team developes and executes the required procedures to effectively handle the incident, propose prevention strategies and updates to policies/systems and log the details.
Part b	In a rotation format, each member of the security team is on a lookout/on call duty to whom incidents are supposed to me reported to. This roation happens every week, and for a given week an

IR-4 What is the solution and how is it implemented?	
	associate from the Security team is on call duty to accept tips and reports. In case of an incident, they are forwarded to the Incident manager and the chief security officer to discuss their handling.
Part c	Learning from historic incidents/logs and improving the functionality and security of the organization is one of the key learning and operating principles of the organization. As discussed in the incident handeling procedures, details which have historically helped in dealing with situations are logged promptly for future associates to work with and gain insights from.

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

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

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

IR-4 (1) What is the solution and how is it implemented?
All users associateds with the organization, both on the intranet and the internet are encouraged and trained to report any notable incidents to the Security Team. This ensures that we have an automated incident surveilence system to notify the authorities instantly given the security team ensures one or the other member is oncall to handle reports. This is also empowered by one of the features of the information security system, that can watermark the data flow and raise alwarms if a packet of data ends up somewhere it should be.

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

The organization tracks and documents information system security incidents.

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

IR-5 What is the solution and how is it implemented?
The Incident monitoring Manager keeps track of all possible incidents including security breaches, any unauthorized access to the databases, malfunctioning of the servers, etc. The manager documents all the details and related to the information including records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. The event logs of the network traffic, data transfers, login attempts associated with the incidents are also documented. The manager receives the incident report from the head of the department where the incident occurred, the person or team who detected the incident, how the detection was carried out, and what might be the possible cause for the incident. After receiving the report the manager documents it in a structured format to note down all possible evidences to make the process of incident handling smoother.

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

The organization:

(a) 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

(b) 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: Incident control manager	
Parameter IR-6(a): 10 days	
Parameter IR-6(b): Incident control Manager	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IR-6 What is the solution and how is it implemented?	
Part a	Whenever an incident is detected like suspicious email, unwanted network traffic, multiple failed login attempts, corruption in databases, etc. the incident should be reported to the incident control manager within 10 days of detection. The manager then sends the report to the federal agencies after thorough analysis of the report and adding specifics of the incidents.
Part b	The incidents need to be reported to the incident control managers, the department dealing with the portion of the system where the incident was detected, Security Administration, and Accounts Manager. The incident manager looks into the incident and holds a meeting with the responsible departments to analyse the issue and possible security threats to figure out what fixes and restoration to ensure prevention of the particular incident.

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

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

IR-6 (1)	Control Summary Information
Responsible Role: Incident Control Manager	
Implementation Status (check all that apply): ✅Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

IR-6 (1)	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

IR-6 (1) What is the solution and how is it implemented?
Incident reporting is automated to eliminate the need for doing it manually that takes man-power and it is time consuming. The application of the automation detects the intrusion detection data, filters it to match the standard report generated. Reports are important to receive technical assistance, statistics collection, increased security awareness, better documentation and to be in-line with organisational policies. The automated incident report has to obey reporting guidelines. The report that is generated must be made to be error free and reliable.

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

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

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

IR-7 What is the solution and how is it implemented?
The Incident Response Assistance includes Helpdesk, assistance systems, forensics services to be used when needed. The assistance includes handling of detection of the threat, its containment,investigation,eradication,recovery and follow-up. The use of physical tools like screwdriver,antistatic protection, analysis laptop that comes with authorized, pre-installed and tested forensic tools that can be used for incident response. The incidence response is documented in a plan that tells the set of actions to b performed to limit the malicious attacks.

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

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

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

IR-7 (1) What is the solution and how is it implemented?
Automated incident response tools are deployed to detect threats by using intelligent decision making ability. They are tasked with stopping malicious IPs from getting into the system by using firewall. The automation tasks of gathering forensics data, disconnecting subsystems that are infected, checking for vulnerabilities will increase the detection and removal of malware. Automated log management are in place to replace the need to check the logs manually. Automated incident response also blocks communication traffic towards and from malicious domain.

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

The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

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

IR-7 (2) What is the solution and how is it implemented?	
Part a	The organisation identifies the internal working members from it's incident response team to work with external providers of information system protection. For our company the Computer Network Center of the Home Land Security provides the external system of protecting the information system. The internal working members work closely with the external providers to establish cooperative relationship. Regular visits to the department and knowledge sharing helps in making the internal members equipped to handle the incident response.
Part b	The organisation identifies incident response team members who are IT professionals having enough experience and background in assessing the security threats and managing it. The team members quickly and efficiently identify the security incidents to regain the control to the system and to thus minimize damage. The team members work with the external security providers to coordinate and communicate the response tasks and events. The updated response plan is communicated with the external providers, to help in preventing future incidents.

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

The organization:

(a) Develops an incident response plan that:

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

(b) Distributes copies of the incident response plan to [*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.

(c) Reviews the incident response plan [*FedRAMP Assignment: at least annually*];

(d) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

(e) Communicates incident response plan changes to [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*]; and

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

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

(f) 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):	

IR-8	Control Summary Information
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization responds to information spills by:

(a) Identifying the specific information involved in the information system contamination;

(b) Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

(c) Isolating the contaminated information system or system component;

(d) Eradicating the information from the contaminated information system or component;

(e) Identifying other information systems or system components that may have been subsequently contaminated; and

(f) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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	

IR-9 (1)	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

IR-9 (2) Control Enhancement (M)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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):	

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

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

13.9. Maintenance (MA)

MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

(b) Reviews and updates the current:

(1) System maintenance policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) System maintenance procedures [*FedRAMP Assignment: at least annually*].

MA-1	Control Summary Information
Responsible Role:	

MA-1	Control Summary Information
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	

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

The organization:

(a) Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

(b) Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

(c) Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

(d) Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

(e) Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

(f) Includes *[Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

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

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

MA-3 Maintenance Tools (M) (H)

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	

MA-3	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

MA-3 (1) Control Enhancement (M) (H)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

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

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

MA-3 (2) Control Enhancement (M) (H)

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

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

MA-3 (3) Control Enhancement (M) (H)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [*FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility*].

MA-3 (3)	Control Summary Information
Responsible Role:	
Parameter MA-3(3)(d):	

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

MA-3 (3) What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

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

The organization:

(a) Approves and monitors nonlocal maintenance and diagnostic activities;

(b) Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

(c) Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

(d) Maintains records for nonlocal maintenance and diagnostic activities; and

(e) Terminates session and network connections when nonlocal maintenance is completed.

MA-4	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

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

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

MA-4 (2) Control Enhancement (M) (H)

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 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)	

MA-4 (2)	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MA-4 (2) What is the solution and how is it implemented?

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

The organization:

(a) Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

(b) Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

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

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

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

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

MA-5 (1) Control Enhancement (L) (M)

The organization:

(a) 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

(b) 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

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)	

MA-5 (1)	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MA-5 (1) What is the solution and how is it implemented?	
Part a	
Part b	

MA-6 Timely Maintenance (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

13.10. Media Protection (MP)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(c) Reviews and updates the current:

(1) Media protection policy [*FedRAMP Assignment: at least every three (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	

MP-2 Media Access (L) (M)

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: Chief Information Officer	
Parameter MP-2-1: Digital and Non-Digital media	
Parameter MP-2-2: System Developer	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MP-2 What is the solution and how is it implemented?
The organisation restricts access to company’s digital and non-digital media to System Development team. Digital media includes flash drives,pendrives,electronic documents,solid state drives,magnetic drives. Non-digital media include paper documents,microfilms,preserved information. The personnel outside of the system development team cannot access the media until they have authorization. Any unauthorized accesses is logged in to the system to analyse the attempt to access the confidential information by unauthorized personnel.

MP-3 Media Labeling (M) (H)

The organization:

(a) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

(b) Exempts [*FedRAMP Assignment: no removable media types*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

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

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

MP-3	Control Summary Information
Responsible Role: System Adminstrator	
Parameter MP-3(b)-1: No removable media type	
Parameter MP-3(b)-2: Not applicable	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MP-3 What is the solution and how is it implemented?	
Part a	All media and IT equipment holding media that the system administrator is in charge of must be marked with the distribution restrictions, handling warnings, and applicable security marks. Federal laws, executive orders, directives, policies, rules, standards, and guidelines are reflected in the marking of information system media. The media of the organization must be labeled in accordance with the system's highest level of categorization to which it is connected. System owners are required to make sure that any media and IT equipment containing media that they are in charge of is labeled, including workstations, servers, thin clients, printers, and copiers. The Security Department keeps an eye on network activity, login attempts, and data transfers in the event logs, also reverify the media on timely basis.
Part b	The media which are non removable are must only be marked if it going out the organisation premises. Such media are only issued when its necessary for the business and should have taken permission from the higher authority. Media that contains information deemed by organizations to be in the public domain or to be publicly releasable often does not need security marks. Information system media are marked in accordance with any applicable laws, policies, rules, standards, and recommendations.

MP-4 Media Storage (M) (H)

The organization:

(a) 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.

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

MP-4	Control Summary Information
Responsible Role: Media Storage Controller	
Parameter MP-4(a)-1: Physical database servers for storing SQL and NoSQL databases, legal papers, hard disks associated with the machines of the customer side employees	
Parameter MP-4(a)-2: On premise locked server rooms, and storage room guarded by security officials and under surveillance	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MP-4 What is the solution and how is it implemented?	
Part a	All the digital data within the information system is stored in cloud servers in SQL, NoSQL databases and file storage space. The example of these data include, biological data of the inmates, convicts, their geographical position data, their personal data, personal information of the customer side employees working in different departments, personal information of the scientists, surveillance footages of the convicts and the former convicts in the outside world. The hard disks associated with machines on which the employees working in the customer side will be kept secured by effective firewalls and antiviruses, security updates and constant monitoring of the event logs of the network

MP-4 What is the solution and how is it implemented?	
	traffic, account logins and data transfers using CloudWatch. Pulse secure VPN will be used for connecting through VPN. The servers would be on premise as it contains data related to homeland security and will be under constant surveillance and guarded by security officials. These rooms will be locked and the key to the room would only be accessed by Media Storage Controller and Security Manager. All the legal documents and physical files about the convicts and former convicts, reports about experiments by the scientists, documentations will be stored in the storage room which will be locked and also be under constant surveillance. The access key will be handed to Media Storage Controller and Security Manager. The cloud service providers would be having access to the servers on premise for maintenance and updates of the software.
Part b	The digital and the non-digital media and data are protected using constant surveillance with CCTV cameras, security officials guardian the storage rooms and server rooms. The physical files are stored in locked safe in the storage rooms. The Security Manager and the Security Department monitors the event logs for network traffic, login attempts, data transfers. The Web Application firewall used is Amazon WAF for securing the cloud based web application. The databases are backed up every day at midnight. The data access are different for different account types depending on the responsibility to ensure no unauthorized access to the high security data. The hard disks in the machines of the customer side employees undergo regular security checks and the systems are kept updated with firewalls and antiviruses. The cloud service provider employees will not have access to any data used by the homeland security. The public data are made accessible from the website. No personal storage devices are allowed on premise and customer side employees are restricted to access any kind of personal cloud storage spaces in the information system. The physical files are accessed from storage rooms only under the permission of the Media Controller Officer and all the files in access will be tracked by the officer. Any discarded, irrelevant, nonessential media is destroyed and made sure that no trace of those exists anywhere in the system to prevent it from going to wrong hands.

MP-5 Media Transport (M) (H)

The organization:

(a) 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/AO.

(e) Maintains accountability for information system media during transport outside of controlled areas;

(f) Documents activities associated with the transport of information system media; and

(g) Restricts the activities associated with transport of information system media to authorized personnel.

MP-5	Control Summary Information
Responsible Role: Security officer	
Parameter MP-5(a)-1: Cloud Buckets	
Parameter MP-5(a)-2: AWS and WinZip encryption module	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ✅ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MP-5 What is the solution and how is it implemented?	
Part a	The company implements ever evolving encryption module of WinZip to protect and encrypt its media for safe storage in transit and transfer. Since the organization heavily relies of cloud nfrastructure, it uses the AWS data-at-rest and data-in-transit encryption techniques that are industry standards for secure storage and retrieval for the cloud buckets. As the situation demands, if a need arises where sensitive data has to be stored in digital or non-digital media, for example in hard disks and papers, the former are ensured to be encrypted and the former are converted to digital form as they serve their purpose and then shredded.
Part b	Information system media are held secure while in-transit out side the controlled areas such as the interne to physical handling, by acknowledgement techniques like# way handshake and securely distributed private key from with in the controlled area. This at times requires the authorized users to be in the controlled network space in order for th receive the private key, and thanks to the state of the art encryption technology the organization uses, the data in transit is impossible to decrypt. To add a further layer of security to this, in order to even attempt to decrypt the data, the attemptee must pass the 3 way handshake.
Part c	May it be digital or non digital media, their status in transit is heavily tracked by the IT team. this ensures collecting digital footprintsof the path it takes over the controlled and un-controlled networks alike. A history of operations and opperands is kept in record with respect to the handling of any media with sensitive information. The latter is also implies to non digital media, which i usually encouraged to be destroyed after they have served their purpose.
Part d	A lot of care is taken to ensure than the media is delivered to the authorized personnel and they have appropriate means to gain access to it. As the encryption renders the media into a binary blob which is seemingly un understandable without the securely transferred private key. This “pickled” nature of the media ensures that it is way lighter, useless without an appropriate encoder, serves no purpose and can mostly cause no loss of data if fallen into wrong hands.

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

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

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

MP-5 (4) What is the solution and how is it implemented?
For digital media transfer, the hard disks are ensures locking and encrypting the data enclosed with AWS encryption which is also implemented in Data-at-rest requirements of the organization. The hardisks are rendered useless unless certain conditions are met. One of them is having access to a private key which is transferred with in the secured/controlled area, i.e, requires the user to be with in the controlled network space or with in the office, and the other mechanism is to acknowledge the right user using three way handshake. And while transferring, non digital media, which is usually very rare, are placed in secured cases with passwords of their own and the papers are sealed within envelopes, to ensure their authenticity. These transfer modes are usually wiped by factory resetting the former and shredding the latter.

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

The organization:

(a) Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

(a) Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-6	Control Summary Information
Responsible Role: Chief Information Officer	
Parameter MP-6(a)-1: All system media	
Parameter MP-6(a)-2: Cryptographic erase and destruction	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MP-6 What is the solution and how is it implemented?	
Part a	The organization sanitises all system media prior to disposal, releasing it out of organisation premises,reusing by adopting sanitisation techniques and procedures that are approved in the organisation. The techniques applies to digital and non digital media. The 24x7 surveillance of the parolees whereabouts and tracking has to be stored in the system using digital media. The data is confidential to the individual rights of the parolee and is only meant for the use of the Homeland Security. Hence the data is to be erased when it goes out of the hands of the Homeland Security.
Part b	The sanitisation techniques and procedures employed by the system developers depends on the criticality of the data that is stored in the media. The location information, video surveillance of the parolee and the persons related to them are extremely critical and to delete this data highest reliable methods have to used, which includes complete physics destruction of the storage media as the last step. The parolees personal identity information stored in the physical documents can be redacted.

MP-6 (2) Control Enhancement (M)

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

MP-6 (2) What is the solution and how is it implemented?
The testing of the sanitisation equipment is conducted by qualified and authorized external federal entities. The test is performed annually to ensure the test equipments are working in optimal performance level. If the performance is not upto the level then the equipment is calibrated and corrected. The test methods adopted are as per the standards complied with Federal agencies. The equipment undergoes quarterly maintenance. The sanitisation procedures are also verified in ensuring the confidentiality of the data in the media storage.

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

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 Summary Information
Responsible Role:	
Parameter MP-7-1:	
Parameter MP-7-2:	
Parameter MP-7-3:	
Parameter MP-7-4:	

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

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

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

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

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

MP-7 (1) is the solution and how is it implemented?

13.11. Physical and Environmental Protection (PE)

PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

(h) Reviews and updates the current:

(1) Physical and environmental protection policy [*FedRAMP Assignment: at least every three (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)	

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

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

The organization:

(a) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

(i) Issues authorization credentials for facility access;

(j) Reviews the access list detailing authorized facility access by individuals [*FedRAMP Assignment: at least annually*]; and

(k) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by:

(1) Verifying individual access authorizations before granting access to the facility; and
(2) Controlling ingress/egress to the facility using [*FedRAMP Assignment: CSP defined physical access control systems/devices AND guards*];

(l) Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

(m) Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

(n) Escorts visitors and monitors visitor activity [*FedRAMP Assignment: in all circumstances within restricted access area where the information system resides*];

(o) Secures keys, combinations, and other physical access devices;

(p) Inventories [*Assignment: organization-defined physical access devices*] every [*FedRAMP Assignment: at least annually*]; and

(q) 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 Summary Information
Responsible Role:	
Parameter PE-3(a):	
Parameter PE-3(a)(2):	
Parameter PE-3(b):	
Parameter PE-3(c):	
Parameter PE-3(d):	
Parameter PE-3(f)-1:	
Parameter PE-3(f)-2:	
Parameter PE-3(g):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

PE-3	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-4 Access Control for Transmission Medium (M) (H)

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 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	

PE-4	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-5 Access Control for Output Devices (M) (H)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

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

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

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

The organization:

(a) Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

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

(c) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

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

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

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

The organization:

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

(b) 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	

PE-8	Control Summary Information
☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-9 Power Equipment and Cabling (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-10 Emergency Shutoff (M) (H)

The organization:

(a) Provides the capability of shutting off power to the information system or individual system components in emergency situations;

(b) Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and

(c) Protects emergency power shutoff capability from unauthorized activation.

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-11 Emergency Power (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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	

PE-12	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-13 (2) Control Enhancement (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PE-13 (2) What is the solution and how is it implemented?

PE-13 (3) Control Enhancement (M) (H)

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	

PE-13 (3)	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PE-13 (3) What is the solution and how is it implemented?

PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

(a) 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

PE-14 (a) Additional FedRAMP Requirements and Guidance:
Requirement: *The service provider measures temperature at server inlets and humidity levels by dew point*.

(b) Monitors temperature and humidity levels [*FedRAMP Assignment: continuously*].

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):	

PE-14	Control Summary Information
☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

PE-14 (2) Control Enhancement (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PE-14 (2) What is the solution and how is it implemented?

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

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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	

PE-16	**Control Summary Information**
□ Not applicable	
Control Origination (check all that apply): □ Service Provider Corporate □ Service Provider System Specific □ Service Provider Hybrid (Corporate and System Specific) □ Configured by Customer (Customer System Specific) □ Provided by Customer (Customer System Specific) □ Shared (Service Provider and Customer Responsibility) □ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PE-16 What is the solution and how is it implemented?

PE-17 Alternate Work Site (M) (H)

The organization:

(a) Employs [*Assignment: organization-defined security controls*] at alternate work sites*;*

(r) Assesses as feasible, the effectiveness of security controls at alternate work sites; and

(s) 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 Responsibility) □ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PE-17 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

13.12. Planning (PL)

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

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

(t) Reviews and updates the current:

(1) Security planning policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Security planning procedures [*FedRAMP Assignment: at least annually*].

PL-1	Control Summary Information
Responsible Role: Security Policy Manager	
Parameter PL-1(a): Security Policy Department	
Parameter PL-1(b)(1): 3 years	
Parameter PL-1(b)(2): Annually	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ✅ Service Provider Corporate ☐ Service Provider System Specific	

PL-1	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific)	

PL-1 What is the solution and how is it implemented?	
Part a	The Security Policy Manager develops and documents all the security planning policies and details about the procedures to implement these policies at organizational level and specific to the different account types in the organization. The generic security policies and procedures include how to plan security threat assessments; how to keep passwords secure and encrypted; no transfer of data to any personal physical or cloud storage or any unauthorized storage; transferring files within the system using the MFT protocol, which is FedRAMP compliant; how to monitor event logs using CloudWatch, what key parameters to check for security threats; how to connect to VPN using credentials and multifactor authentication using Okta Verify, which is FedRAMP compliant; how to securely access biological, geological, and personal data of inmates and ex-offenders, etc. There are also role specific policies and the limitations of these roles mentioned in the documentation that avoid access conflicts, which may lead to security casualties. These documents are distributed to all accounts in the information system and network traffic. Account activity logs are monitored by the Accounts Manager and Security Policy Manager to ensure every activity is in accordance with the security policies and procedures.
Part b	The security policies are updated every 3 years by conducting a meeting between higher authorities, policy manager, network security department, and account department to keep these policies in accordance with the changes in federal laws, executive orders, directives, regulations, policies, standards, and guidance. There are also emergency meetings for policy reviews and updates when there is a potential security threat and the policies need to be updated to reflect the correction of flaws that resulted in the security threat. The procedures are updated annually to keep the system on track with the updates and patches in the security software and technologies being used in the system. These reviews and updates can even occur in case of any security threats which requires the There are procedures to be corrected that lead to the security threat, and the procedures and policies are well tested with Vulnerability Scanning, Security Scanning, Penetration testing, Risk Assessment, Security Auditing, Ethical Hacking, and Posture Assessment.

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

The organization:

(a) Develops a security plan for the information system that:

(3) Is consistent with the organization’s enterprise architecture;
(4) Explicitly defines the authorization boundary for the system;
(5) Describes the operational context of the information system in terms of missions and business processes;
(6) Provides the security categorization of the information system including supporting rationale;
(7) Describes the operational environment for the information system and relationships with or connections to other information;

(8) Provides an overview of the security requirements for the system;
(9) Identifies any relevant overlays, if applicable;
(10) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
(11) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

(u) Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

(v) Reviews the security plan for the information system [*FedRAMP Assignment: at least annually*];

(w) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

(x) Protects the security plan from unauthorized disclosure and modification.

PL-2	**Control Summary Information**
Responsible Role: Security Architect	
Parameter PL-2(b): All users connected via the Intranet, including managers, Information security, audit and IT personnel.	
Parameter PL-2(c): Anually	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PL-2 What is the solution and how is it implemented?	
Part a	Security plans should be reviewed and approved by the managers and administration staff from all the departments to ensure that the security design does not interfere with the organizational architecture and vice versa. To achieve this, the Security architect has to ensure he understands the functional architecture of the organization and is able to communicate his ideas with the aforementioned jury who is responsible for the reviewing.
Part b	The authorization boundary of the security system expands to all the components connected to the

PL-2 What is the solution and how is it implemented?	
	private secure network, devices connected to the network, multi factor authentication applications, internal homegrown tools and ports to the external tools used by the organization. It is the responsibility of all the clients to be aware of and respect the terms and conditions presented by the system and its boundaries.
Part c	The operational context of the security system is heavily centered around controlled, secure and limited information flow to establish and maintain the principles of least privilege among different entities with in the security systems authorization boundary.
Part d	The information system's security applies to two major categories, one to establish and secure the flow of information, followed by firewall protection from the external threats. The former is governed and orchestrated using a Information Security system, which inculcates security training, logging, security system review and update and the former includes standard and secure firewall security system that ensure overall protection from external threats and intruders.
Part e	The operational environment of the security system extends to the private network and the virtual private network used by the clients. The information system supports a controlled information flow to and from the endpoints as prescribed in the architecture and there also lies a layer of security just above the abstraction level of the information system. The information system and the security system are well encapsulated in a sense that one acts as a mere external construct and protective layer which does not restrict or influence the system's architecture. Then there is the database information which is one of the endpoints to the system, and is connected to it and communicates with it securely via encryption.

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

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: Rotating responsibility of the Security Team	
Parameter PL-2(3): IT and Security Team	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)	

PL-2 (3)	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PL-2 (3) What is the solution and how is it implemented?
Security awareness and training activities among the organization wide entities centered around and organized by the security and IT team with an agenda to preserve, improve and propagate the quality of security. Here, in additional to major topics relating to security, quality of life enhancements and minor requests by clients from different entities. By incorporating these events into company's culture enables access to a platform for clients from various other entities to express their concerns and suggestions with regards to the security policies and system. These sessions can also be used to encourage awareness, training and right knowledge on do's and don'ts of our security system.

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

The organization:

(a) 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;

(a) 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;

(b) Reviews and updates the rules of behavior [*FedRAMP Assignment: at least every three (3) years*]; and

(c) 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: Security Manager	
Parameter PL-4(c): Every 1 year	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

PL-4	Control Summary Information
☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from a pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PL-4 What is the solution and how is it implemented?	
Part a	Rules of behavior should be in place within organizations to guarantee total information security. These guidelines are intended to make users aware of their accountability for their actions, roles, and duties. Users must comprehend that it is their obligation to protect the data they have on their computers. Users are expected to comprehend the rules and follow them at all times as part of the security culture. The company erroneously believes that everyone in a security-related function is aware of best practices and adheres to them. Organizations should work hard towards security by carrying out awareness campaigns, advertisements, and sanitizing personnel towards maintaining a healthy and secure environment.
Part b	Users need to be extra cautious because they are gaining access to sensitive information. Users must sign a form acknowledging that they understand their responsibilities with regard to information security before being allowed access to the information. The Accounts Manager monitors account activity records to ensure that all activities adhere to security standards and rules.
Part c	Everyday, there are people who toil to find loopholes in the hard work put in by the organization. So, the organization will review and update the rules of behavior to keep up with the pace. The review and update process is being conducted to strengthen security and decrease the frequency of breaches. Higher management, the security department, and the account department meet once a year to discuss how to keep these rules up to date with new federal laws, regulations, policies, standards, and recommendations.
Part d	Every employee will read, comprehend, and sign the acknowledgement form once more after the rules of behavior have been reviewed and updated. The review and update procedure is being carried out to improve security and reduce the number of security breaches.

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

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

PL-4 (1)	Control Summary Information
Responsible Role: Security Manager	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented	

PL-4 (I)	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PL-4 (I) What is the solution and how is it implemented?
The usage of social media and networking sites is strictly prohibited within the corporation, as stated in its strict rules of behavior, as the majority of attacks take place on social media, which is used by everyone in the company. All devices, including networks, computers, email, and other informational assets, may be observed, recorded, and audited. Users must be informed that organization data is not permitted to be disclosed on social media per the rules of behavior. Social media cannot be used to collect non-public information. To make sure that all activities follow security guidelines and standards, the account manager keeps an eye on account activity logs.

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

The organization:

(a) 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;

(y) Reviews and updates the information security architecture [*FedRAMP Assignment: at least annually or when a significant change occurs*] to reflect updates in the enterprise architecture; and

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

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

(z) 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: Senior Information Security Officer	
Parameter PL-8(b): Annually	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☑ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PL-8 What is the solution and how is it implemented?	
Part a	The organization develops security and privacy architectures for the system. The architecture specifies requirements to protect the confidentiality, availability, and integrity of the organization by restricting unauthorized access and encrypting information and the data of the company. The architecture describes the processing of PII by collecting and identifying the PII data of the company,the location where it is stored; classifying the sensitive information; forming usage policies; and backing it up. The security architecture is integrated by using relevant components of IT, including hardware and software systematically into the enterprise architecture. The organisation assumes that all the roles working under security understand and follow safe practices.
Part b	The system architect reviews and updates the information security architecture annually to reflect updates in the enterprise architecture. The accuracy of the current network, inspecting audit logs,validating current policies and analyzing vulnerabilities are tasks under review, which is updated in the architecture document every year. The objective of doing the review and update is to provide increased security and reduce the number of breaches.
Part c	Information security architecture changes is reflected in the security plan to be consistent with the organization's security plan, which is part of enterprise architecture. The security architecture description, functionalities, interfaces,protection mechanisms, role based privileges are part of the architecture. The system security architecture undergoes changes and updates around the system development lifecycle, which are updates in security plan, security concept of operations, and organizational procurements and acquisitions.

13.13. Personnel Security (PS)

PS-1 Personnel Security Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(aa) Reviews and updates the current:

(1) Personnel security policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Personnel security procedures [*FedRAMP Assignment: at least annually*].

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

PS-2 Position Categorization (L) (M)

The organization:

(a) Assigns a risk designation to all positions;

(a) Establishes screening criteria for individuals filling those positions; and

(b) Reviews and revises position risk designations [*FedRAMP Assignment: at least every three (3) years*].

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

PS-2 What is the solution and how is it implemented?	
Part a	The Security Manager assigns risk designation to all positions in every department for determining the level on how the position is prone to security threats, what data those positions have access to and what kind of security measures have been implemented in safeguarding the access from those positions. The Security manager reviews and analyzes activities, event log, data transfer, type of data access, responsibilities, screening policies, and network traffic from those accounts and determines the risk designations.
Part b	The Security manager establishes screening criteria for all the positions to which he assigns risk designations. The position screening includes security clearances, and the individuals in the position are provided mandatory training for accessing the assigned resources and general security measures taken to ensure safety like not sharing access credentials, ways on using VPN using Pulse Secure, encrypting data using Azure Data Encryption when sending it over network be it secured and unsecured. Also, the account activities are constantly monitored by the Security Manager. The individuals in the positions need to complete these trainings and pass a test with at least 80% to qualify for training certification.

PS-2 What is the solution and how is it implemented?	
Part c	The Security Manager reviews and updates the risk designations annually by holding a meeting with the Accounts manager, security department and system administrator by analyzing the data transfers, occurrence of any suspicious activity in any position, reviewing statements from the positions involving in any suspicious activity, or getting affected by one, going through the system logs and event logs from SolarWinds Event log Analyzer, tcp dumps, etc. Upon getting affected by an unplanned risk, the Security manager performs the reviews to cope with the risk and ensure prevention of the risk occurring.

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

The organization:

(a) Screens individuals prior to authorizing access to the information system; and

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

PS-3	**Control Summary Information**
Responsible Role: Security Screening Manager	
Parameter PS-3(b): Reinvestigation is required during the 5th year, secret security clearance is required during the 10th year and for confidential security clearance during the 15th year. For individuals accessing high security data, a security screening is required every year.	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PS-3 What is the solution and how is it implemented?	
Part a	The Security Screening Manager plans the screening of individuals having access to the information system be it within the organization or outside of organization. The manager reviews through the federal laws, executive orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations and plans and documents the screening. The individuals accessing the resources with lowest risk threats and who are working as interns do not require a security clearance and all the rest individuals are subjected to the security clearance for their positions.
Part b	All the users apart from the temporary ones and the ones who access low level security data are not subjected to rescreening but the rest are subjected to rescreenings mentioned in the parameters. The individuals having access to the most secured and high security data are subjected to annual screening by performing internal audits on the account event logs for those accounts, to check whether their activities are aligned with the standards and policies, whether they were subjected to any threat, what data are getting accessed the most from those accounts, the encryption of the data, how the security measures are working on their end, etc.

PS-3 (3) Control Enhancement (M) (H)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(bb) Satisfy [*FedRAMP Assignment: personnel screening criteria – as required by specific information*].

PS-3 (3)	**Control Summary Information**
Responsible Role: Data Protection Officer	
Parameter PS-3 (3)(b): Security Clearance and mandatory security training	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PS-3 (3) What is the solution and how is it implemented?	
Part a	The data protection officer ensures that all the users having access to the information system have valid access authorizations and it is aligned by the assigned official government duties. The authorization measures are different for different account types and depend on the responsibility and the level of security on the data they are accessing. For on premise access of physical data like files, the individual has to get permission from the Data protection officer to access the storage room with their biometrics like fingerprint. When accessing high security files, the individuals must enter their credentials along with the multifactor authentication to access them and the access is in constant monitoring by the Data protection officer. The officer also goes through the encryption of the data at rest to ensure the encryption is secured and no information can be retrieved out of it without specific keys. The data protection officer along with the Security Screening Manager ensures all the individuals are compliant with the security clearances required for their positions.
Part b	The data protection officer along with the Security Screening Manager ensures all the individuals are compliant with the security clearances required for their positions and they are certified by the security training which are general as well as responsibility specific. They also make sure the individuals are compliant with the rescreening and the individuals need to provide a show cause in case of any issues with these rescreenings. The mandatory security training also requires the individuals to pass with 80% to be considered as certified by training and get access to the information system for accomplishing their assigned responsibilities.

PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

(a) Disables information system access within [*FedRAMP Assignment: same day*];

(a) Terminates/revokes any authenticators/credentials associated with the individual;

(b) Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

(c) Retrieves all security-related organizational information system-related property;

(d) Retains access to organizational information and information systems formerly controlled by terminated individual; and

(e) Notifies [*Assignment: organization-defined personnel or roles]* within [*Assignment: organization-defined time period*].

PS-4	Control Summary Information
Responsible Role: Information Technology Associate	
Parameter PS-4(a): 12 Hours	
Parameter PS-4(c): Associate password and acknowledgement of proper knowledge transfer	

PS-4	Control Summary Information
Parameter PS-4(f)-1: Chief Information Officer	
Parameter PS-4(f)-2: 24 hrs	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PS-4 What is the solution and how is it implemented?	
Part a	Changing access control settings for all the user accounts with in 12 hours of termination employment. The organization expects to freeze the accounts for upto 7 days of the termination of employment , in case the organization needs access to details from their account, related to missed out components in the knowledge transfer or general queries.
Part b	As the accounts are frozen, the terminated employee looses all access points to organization relation entitites, rendering their , “principle of least privilege” nature of access to principle of no privilege. The user looses all the privileges, organization related benefits and entities.
Part c	The exit interviews at the organizatin generally include a series of questions to get documentation done for a systematic knowledge transfer for the replacement, gain an in depth overview of the employee’s time here at the organization, get some notable insights on the employee’s time at the organizartion and get some security related formalities addressed.
Part d	The organization greatly encourages exit interviews to promote culture, by getting honest feedback on how they felt working here, knowledge transfer and documentation to ensure the projects and operations the employee has been working on can be resumed seamlessly by their replacement or teammembers momentarily. This ensure least employee termination and operation recommencement costs.
Part e	The organization then retrieves information security related properties like VPN access, physical digital media carriers, work station and organization provided access to entities, both internal and external. The orgainzation also asks users to sign non discolcure agreement over organization related data and data processing, requests the individual to submit organization related information.
Part f	The organisation would inform Chief Information Officer about the termination of the employment of an employee within 24 hrs. The notification would be sent through email. Depending on the employment type, the notification would also be given in-person with additional details on what measures are taken to ensure there is no scope for data breach. Robust and comprehensive security practices in terms of applications ,firewalls and sensitive systems are put in place for protection.

PS-5 Personnel Transfer (L) (M)

The organization:

(a) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

(a) Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];

(b) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

(c) Notifies [*Assignment: organization-defined personnel or roles*] within [*FedRAMP Assignment: within five days of the formal transfer action (DoD 24 hours)*].

<table>
<tr><th>PS-5</th><th>Control Summary Information</th></tr>
<tr><td colspan="2">Responsible Role: Chief Information Officer</td></tr>
<tr><td colspan="2">Parameter PS-5(b)-1: Transfer</td></tr>
<tr><td colspan="2">Parameter PS-5(b)-2: 24 hrs</td></tr>
<tr><td colspan="2">Parameter PS-5(d)-1: ID Management Manager</td></tr>
<tr><td colspan="2">Parameter PS-5(d)-2: 24 hrs</td></tr>
<tr><td colspan="2">Implementation Status (check all that apply):
✅ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable</td></tr>
<tr><td colspan="2">Control Origination (check all that apply):
☐ Service Provider Corporate
Service Provider System Specific
☐ ✅Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization</td></tr>
</table>

<table>
<tr><th colspan="2">PS-5 What is the solution and how is it implemented?</th></tr>
<tr><td><b>Part a</b></td><td>The organisation reviews the need to transfer certain employees for a different roles that is required in a different department under the same organisation. Transfer of the personnel will retain their</td></tr>
</table>

PS-5 What is the solution and how is it implemented?	
	association with organisation with transfer and changes in their duties. On those occasions, the information systems have to consider this change and reflect in their systems, so that the risks that comes with such changes is addressed. The current access has to be modified,disabled, or removed in order to protect resources,data and facilities.
Part b	The higher level management - the Senior Homeland Officer, Chief Security officer, and Secretary of Homeland, when decide to transfer the employee, would initiate the process of transfer. Such initiation would start the process after 24 hrs of the decision being made. The criticality of the data handled is high, and hence depending on the role that is being transferred, and the kind of duties they would discharge, the change of access to the data and facilities should be immediately performed, to avoid data breach.
Part c	The System Administrator will modify the access of the employee that is being transferred, after knowing about the decision to transfer. The changes performed for the access of the employee depends on what their previous roles was and what their new roles is going to be. The accesses related to human resources,management,administrative and security would undergo changes. All the accesses pertaining to networks,computers,mobile devices and applications and physical locations access to buildings and rooms are updated.
Part d	The decision of transfer of the employee, after being made by the higher level authorities at the management level should also be followed by the changes in the access of the employee in the system level, within 24 hrs of receiving such notification The changes in the access of the employee should follow the IT policy of the company. The process have to be coordinated with Information System Security Officer and should be authorized by the Authorizing Official, before informing to the Chief Information Officer which would be the last step of the process.

PS-6 Access Agreements (L) (M)

The organization:

(a) Develops and documents access agreements for organizational information systems;

(b)Reviews and updates the access agreements [*FedRAMP Assignment: at least annually*]; and

(cc) 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: Chief Information Officer	
Parameter PS-6(b): Annually	

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

PS-6 What is the solution and how is it implemented?	
Part a	The access agreement will be documented by the chief information officer. The agreement specifies the proper access and use of the covered data as well as the procedures for obtaining unapproved access and usage. Every employee of the company must sign this document, which confirms that they have read, comprehend, and agree to adhere by the restrictions placed on organizational information systems to which access is permitted. Nondisclosure, permissible usage, conduct, and conflict-of-interest agreements are all included in the Access Agreement.
Part b	The CIO examines and revises the access agreement every year in a meeting with the accounts manager, security team, and system administrator. They do this by looking at data transfers, the occurrence of any suspicious activity in any position, reading statements from those positions involved in that activity or affected by it, looking through system logs and event logs from SolarWinds Event log Analyzer, TCP dumps, etc. Performing the review and update has the goal of maintaining the pace. Each employee is required to read the full access agreement again and sign it.
Part c	Each time a new employee joins the business, they must sign the access agreement. This agreement will specify the employee's level of access to the company. An electronic signature may be used to formally sign the agreement. The access agreement will be reviewed every year, and any necessary changes will be thoroughly documented. Changes will be made in accordance with the needs. After the agreement has been reviewed and amended, each employee will read, understand, and sign it once more. To increase security and decrease the frequency of security breaches, the review and update procedure is being carried out.

PS-7 Third-Party Personnel Security (L) (M)

The organization:

(a) Establishes personnel security requirements including security roles and responsibilities for third-party providers;

(a) Requires third-party providers to comply with personnel security policies and procedures established by the organization;

(b) Documents personnel security requirements;

(c) 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

(d) Monitors provider compliance.

PS-7	**Control Summary Information**
Responsible Role: Security Manager	
Parameter PS-7(d)-1: Notify the Security Manager	
Parameter PS-7(d)-2: Same Day	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PS-7 What is the solution and how is it implemented?	
Part a	When third parties access the data, the Security Manager maintains the least permissible level. Only specific files and folders can be read, written to, or executed by third parties. Only the fundamental operations necessary to keep the system running are permitted for the system. Given that each Third Party's responsibilities are specified, any tasks that fall outside the purview of the Third Party's responsibility will be canceled. Only the permission levels necessary for each obligation to complete its duties will be granted. The system logs any attempts by a Third Party to access restricted content and later reviews those logs. The Security Manager verifies the Third Party's authenticity by investigating all of their credentials and history before granting authorization. After that, they will be granted permission to take certain actions. Their access is watched to see how they use it.

PS-7 What is the solution and how is it implemented?	
Part b	Due to the fact that third parties are not employees, organizations have separate security procedures for them. Contractors and other businesses that design information systems, offer IT services, manage networks and security, and provide outsourced applications are considered third parties. The set policies and procedures of the organization secure the system control by each form of third-party account and the methods for control enhancements. The policies will also include training on the resources that can be accessed from each account and the requirements for using the systems, such as 2-step authentication for login and password changes every three months. In a document that will be distributed to all outside parties, the documentation expert frames the policies and processes.
Part c	To keep things safe and secure, the security manager has been quite active. Every third party connected to the organization has their personal information stored by the security manager. The credentials, badges, or system rights that have been granted by organizations are included in this data. The request for the creation of privileged accounts with authentication is approved by the management. The initial authentication for network access would be a password, and after that it would be necessary to supply a valid token that would be produced on their own devices. The accesses will be continuously watched. These data are used to create reports, which are then given to the security management department.
Part d	The third-party would notify the security manager of the employee's termination or transfer on the same day. The notification would be issued via email and include details regarding the responsibilities, roles, and types of credentials or privileges connected with the transferred or terminated personnel that security-related characteristics regarded the transfers and terminations to be reportable. Depending on the type of employment, the notice may also be made in person and include further information on the steps taken to guarantee that there is no chance of a data breach. Access to the particular third-party employee will elicit and then limit access to sensitive company data.
Part e	The security manager monitors all the accounts and the activities of every third party. If any activity is noticed that is not as per the standard and rules of the company, the manager documents all the details and related to the investigation & make a report for non-compliance. The department reviews and tallies them with the control policies and standards mentioned in the agreement documentation. Further, a chance will be given to the third party to make their point, if the third party fails to proof the valid reason behind the non-compliance, a penalty will be imposed as per the agreed agreement.

PS-8 Personnel Sanctions (L) (M)

The organization:

(a) Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and

(b) Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment:*

organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-8	Control Summary Information
Responsible Role: Chief Information Security Officer	
Parameter PS-8(b)-1: Chief Information Officer	
Parameter PS-8(b)-2: 24 hrs	
Implementation Status (check all that apply): ✅Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

PS-8 What is the solution and how is it implemented?	
Part a	The organisation sanctions are in accordance with Executive orders,Federal laws,diretives,regulations,policies,standards and guidelines. Sanctions are issued to the employees who fail to comply to the organisational compliance program. The sanctions can range from as low as being subjected to disciplinary action of lowest kind to termination of the employee. The non-employee staff of the organization if found to violate company's privacy policies would be disciplined.
Part b	The decision to sanction on a certain employee will be taken by senior officials of Homeland security - Secretary, Senior Security Officer and Chief of Security. The decision would be passed onto Chief Information Officer within 24 hrs of taking the decision, who would terminate all the access related to security,data,human resource,management and administration. All the physical access to buildings,rooms,network room and maintenance, data centers, control room would be revoked.

13.14. Risk Assessment (RA)

RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(3) A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(4) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

(dd) Reviews and updates the current:

(1) Risk assessment policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Risk assessment procedures [*FedRAMP Assignment: at least annually*].

RA-1	Control Summary Information
Responsible Role:	
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	

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

The organization:

(a) Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(b) Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

(c) Ensures the security categorization decision is reviewed and approved by the AO 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

RA-3 Risk Assessment (L) (M)

The organization:

(a) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

(ee) Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*FedRAMP Assignment: security assessment report*]];

(ff) Reviews risk assessment results [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*];

(gg) Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

(hh) Updates the risk assessment [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

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

RA-3 (d) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-3	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

The organization:

(a) 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.

(ii) 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;

(jj) Analyzes vulnerability scan reports and results from security control assessments

(kk) Remediates legitimate vulnerabilities; [*FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery*], in accordance with an organizational assessment of risk; and

(ll) Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-5 (e) Additional FedRAMP Requirements and Guidance:

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

RA-5 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Vulnerability Scanning Requirements
https://www.FedRAMP.gov/documents/

RA-5	Control Summary Information
Responsible Role: Risk Assessment officer	
Parameter RA-5(a): monthly	
Parameter RA-5(d): High Risk Vulnerabilities - 15 days, Moderate Risk Vulnerabilities - 30 days, Low Risk Vulnerabilities - 60 days	
Parameter RA-5(e): Vulnerability Assessment Analyst	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ✅ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

RA-5 What is the solution and how is it implemented?	
Part a	The vulnerability scanning of the operating system, web applications, web application firewalls, application servers, database servers, hardware resources like networked printers, scanners, etc. are performed monthly and when any new vulnerability has been identified and reported. An external independent assessor also performs vulnerability scanning on the above mentioned resources annually in order to spot vulnerabilities that might have been missed by the internal scanning. The network traffic and data transfers from different account types are logged and monitored using SolarWinds Event Log Analyzer tool which is fedRAMP compliant. These logs help to identify the vulnerabilities and report them to the risk assessment officer to perform an immediate vulnerability scan on the resource subjected to the vulnerability that was spotted in the logged events. Every end of the month, vulnerability scan is performed with takes atleast 2 days to complete, which includes binary, static, dynamic analysis of the applications, and usage of various tools like web-based application scanners, static analysis tools, binary analyzers and code reviews for all the commits and pushes added that particular month by the risk assessment department. On detection of any vulnerability, a report is generated with the test cases and action performed and their respective outcome from the information system resources and sent to the system administrator and corresponding department for fix or further explanation. The respective department have to respond within 72 hours of the report generation with explanation or rectification measures to counter the vulnerability.

RA-5 What is the solution and how is it implemented?	
Part b	All types of vulnerability scanners are employed to perform a full vulnerability scanning, which includes network-based and application scanner namely, GFI Languard to scan network and web application that can automatically deploy patches across multiple operating systems, third-party applications, and web browsers, host-based, database and wireless scanners scanners namely, ManageEngine Vulnerability Manager Plus which protects every endpoint—workstations, laptops, servers, virtual machines, web servers, and databases; gains unified, continuous visibility of your distributed IT irrespective of endpoints' whereabouts; automatically detect vulnerabilities, misconfigurations, risky software, patch vulnerabilities and fix misconfigurations with the click of a button; spot zero-day vulnerabilities and apply mitigation work arounds; automate and customize patching for Windows, macOS, and Linux based on organization needs; provides test for vulnerabilities as per CWE and NVD; provides view of CVSS and security posture with near real-time dashboards. The code reviews are performed by the risk assessment department at the end of the month to check compliance with standards, enumerating platforms, software flaws, and improper configurations. Analysis such as static analysis, dynamic analysis, binary analysis are performed using BitBlaze. Nmap and RapidFire Tools' Inspector 2 is used for port, protocol and services scanning. They check all the ports on any device connected to a network including servers, desktops, laptops, virtual machines, mobile devices, firewalls, switches and printers. There are monthly red team testing for vulnerabilities. Vulnerabilities reported from these tools are sent to the system administrator and the respective departments where the vulnerabilities have been detected for rectification or explanation.
Part c	The reports of the vulnerabilities generated from GFI Languard, Nmap, BitBlaze, SolarWind Event Log Analyser, RapidFire Tools' Inspector 2 and ManageEngine Vulnerability Manager Plus are analysed to determine the root cause of vulnerability and the areas where the effect can spread and possible remedial solution to the problem. A formal report is made after the review and analysis by the risk assessment department and sent to the System Administrator and respective departments subjected to vulnerabilities and they are given 72 hours to come up with an explanation or rectification measures against the vulnerabilities, which might include production code modifications, update of security softwares, configuration change of these softwares, update of encryption protocols, explanation, etc.
Part d	The remediation of legitimate vulnerabilities are undertaken with 15 days for High risk, 30 days for Moderate risk, and 60 days for Low risk. Our system is highly data sensitive, withholding with itself data of crime and parolees, which can affect millions of Americans, hence they are ensured to be kept safe, hence the timeline used for the remediation in the vulnerability management process is very tight. We are compliant with Cybersecurity and Infrastructure Security Agency's (CISA) BINDING OPERATIONAL DIRECTIVE 19-02 - VULNERABILITY REMEDIATION REQUIREMENTS FOR INTERNET-ACCESSIBLE SYSTEMS, to mitigate the risks associated with monitoring, tracking parolee's real time location and activities and handling of the systems that store the parolees real time data and keep logging their activities information. Our Vulnerability scanning tools - Accunetix,beSecure,FrontLine scans all the IPs belonging to Homeland Security Department, and associated third party websites. After the scanning of the vulnerabilities, they are prioritised using Snyk - cloud native application security platform, to fix it. These vulnerabilities are categorised under High risk, Moderate risk and Low risk. The High risk priorities, are fixed immediately by patching or upgrading, the moderate and low ones are blocked, as the immediate step, and are planned under monthly remediation plan to fix it.
Part e	The monitoring of the vulnerabilities is continuous process happening over entire Software Development Life Cycle (SDLC). The vulnerabilities are received from automated vulnerability testing tools - Software Composition Analysis (SCA) tools - BlackDuck, Snyk, White-box static application security tools - SpectralOps, Snyk. The summary of the vulnerabilities got from scanning tools is given

RA-5 What is the solution and how is it implemented?	
	to Vulnerability Assessment Analyst, who has the knowledge of Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code,buffer overflow, and cross-site scripting. The Analyst analysis the vulnerability and configuration data by using the source code review and logic like fuzzing and nmap. They share meaningful insights based on the context of our system monitoring and tracking parolees who are out, and provide suggestions to improve our vulnerability management process relevant to confidentiality, integrity, availability, authentication, non-repudiation.

RA-5 (1) Control Enhancement (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

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

RA-5 (1) What is the solution and how is it implemented?
Vulnerability scanning identifies weaknesses in the system and softwares running on it, to ensure the overall system is safe from breaches and exposure of sensitive data. The challenges to identify these vulnerabilities manually, is overcome with the help vulnerability scanning tools that identify and create inventories for all system connected over the network. Our tools proactively scan Operating systems (Windows 10 and higher, macOS 10.11 and higher, Linux 4 and higher), enterprise applications (Wokiva, Kronos, SAP US Federal Govt, Accela), web browsers (Google chrome,Microsoft Edge, Safari), end-user (parolee) applications (the sensor software that the parolee should always keep ON for tracking data that is continuously sent to the Homeland Department. The softwares are patched and re-configured. For scanning networks - SolarWinds (to optimize IP discovery), Acunetix (Weak SNMPs misconfigurations and weak TLS/SSL ciphers), OpenVAS (Advance task guidance). For scanning systems - FrontLine(Cloud native SaaS security platform for digital defense) are used.

RA-5 (2) Control Enhancement (M) (H)

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*FedRAMP Assignment: prior to a new scan*]].

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

RA-5 (2) What is the solution and how is it implemented?
The organization uses Sentinel, security tool for vulnerability assessment, developed by WhiteHat Security which is scheduled to be conducted once every 30 days. Under special circumstances, we conduct additional scans with the in the possibility range and vicinity of an anticipated incident, vulnerability or even a report/tip on a potential threat. Members from the Risk Assessment team are trained semi annually on the utilities, functionalities and dependencies of the tool. Currently, we are using the latest version 9.0.0, with each new release, the the tool attempts to encompass and address various new vulnerabilities like HTTP response splitting, routing detour, cross site scripting and so on.

RA-5 (3) Control Enhancement (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

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

RA-5 (3) What is the solution and how is it implemented?
The organization employs vulnerability testing for all the code base and components in production and active usage. Before the users commit any product to deployment, their commits are assessed and checked for any vulnerabilities, potential security loophole, that includes using outdated software components with potential security holes, lint, security components with a bad history of security failures, does not comply with the programming procedures or coding style of the organization. This ensures that clean building blocks are used in production which is enabled by using codefresh, a go to tool for maintaining securing progression and conducting vulnerability checks which works hand in hand with sentinel with in the source control.

RA-5 (5) Control Enhancement (M) (H)

The organization includes privileged access authorization to [*FedRAMP Assignment: operating systems, databases, web applications*] for selected [*FedRAMP Assignment: all scans*].

RA-5 (5)	Control Summary Information
Responsible Role: Risk Assessment officer	
Parameter RA-5(5)-1: Operating systems, Databases, Web applications	
Parameter RA-5(5)-2: All the access scans	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned	

RA-5 (5)	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☑ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

RA-5 (5) What is the solution and how is it implemented?
The company utilizes the security feature known as "privileged access management," or PAM, which enables companies to oversee and keep an eye on the behavior of privileged users. By monitoring privileged access attempts and alerting the security team to any questionable activity, PAM solutions can add an extra layer of security. This can assist firms in maintaining a thorough audit trail to satisfy internal and external compliance needs when combined with reporting features. In other circumstances, the vulnerability scanning process may be more intrusive, or the system component being scanned may contain sensitive or restricted information, such as personally identifiable data. Greater thoroughness in vulnerability assessment is made possible and the sensitive nature of such scanning is protected by privileged access authorisation to certain system components. When a vulnerability is found, a report detailing the test cases, actions taken, and results are generated from the information system resources and forwarded to the system administrator and relevant department for repair or more information.

RA-5 (6) Control Enhancement (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

RA-5 (6)	Control Summary Information
Responsible Role: Risk Assessment officer	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	

RA-5 (6)	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ✅ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

RA-5 (6) What is the solution and how is it implemented?
The business makes use of an end-to-end vulnerability management solution. This vulnerability management software for businesses focuses on priority and includes integrated patching and vulnerability report comparison. This continuously scans endpoints for newly discovered or known vulnerabilities. The business makes use of Security Content Automated Protocol (SCAP) scanning technologies to find vulnerabilities by using the Open Vulnerability Assessment Language (OVAL) and the Common Vulnerabilities and Exposures (CVE) naming system give more places to look for vulnerabilities that need to be scanned using End-to-End Vulnerability Management, which quickly finds flaws in configuration, dangerous applications, and vulnerabilities. Later, examining numerous vulnerability scans over time can assist detect attack patterns and identify trends in system vulnerabilities.

RA-5 (8) Control Enhancement (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

RA-5 (8) Additional FedRAMP Requirements and Guidance:

Requirement: This enhancement is required for all high vulnerability scan findings.

Guidance: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

RA-5 (8)	Control Summary Information
Responsible Role: Security and DevOps Engineer	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ✅ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

RA-5 (8)	Control Summary Information
☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ✅ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

RA-5 (8) What is the solution and how is it implemented?
The organization uses a combination of a python library Slogger and logging facility provided by the codefresh. Currently, the organization has trained its associates who participate in deploying and merging directly to production on the in and outs of using slogger 1.2.1 and codefresh, for their source control and deployment procedures. Codefresh uses extensive logging mechanism which is built in that categorizes security issues in three categories, based on historic vulnerability reports on the severity or range of the risk posed into high, moderate and an "easy fix". developers can quickly asses these registers and logs to fix their issues before they win deploy their build to the production, so this mode of mitigation helps a lot in preventing a problem without even giving a chance. The slogger can be really helpful; whilst in a developing environment as it gives the users a quick historic report of incidents during the development life cycle, the users are encouraged to understand the documentation of slogger to fully leverage its utility and always work in tandem with the organization's core values to always learn from the past to improve the future, avoid risks and block vulnerabilities.

13.15. System and Services Acquisition (SA)

SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

(a) Reviews and updates the current:

(3) System and services acquisition policy [*FedRAMP Assignment: at least every three (3) years*]; and

(4) 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	

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

The organization:

(a) Determines information security requirements for the information system or information system service in mission/business process planning;

(b) Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

(c) Establishes a discrete line item for information security in organizational programming and budgeting documentation.

SA-2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply):	

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

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

SA-3 System Development Life Cycle (L) (M) (H)

The organization:

(a) Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;

(b) Defines and documents information security roles and responsibilities throughout the system development life cycle;

(c) Identifies individuals having information security roles and responsibilities; and

(d) Integrates the organizational information security risk management process into system development life cycle activities.

SA-3	Control Summary Information
Responsible Role:	
Parameter SA-3(a):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

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

SA-3 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

(a) Security functional requirements;

(b) Security strength requirements;

(c) Security assurance requirements;

(d) Security-related documentation requirements;

(e) Requirements for protecting security-related documentation;

(f) Description of the information system development environment and environment in which the system is intended to operate; and

(g) Acceptance criteria.

SA-4 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process).

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.
See https://www.niap-ccevs.org/Product/

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-4 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	

SA-4 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

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

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

SA-4 (2) Control Enhancement (L) (M)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*FedRAMP Selection (one or more): to include security-relevant external system interfaces, and high-level design*]; [*Assignment: organization-defined design/implementation information*] at [*Assignment: organization-defined level of detail*].

SA-4 (2)	Control Summary Information
Responsible Role:	
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):	

SA-4 (2)	Control Summary Information
☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-4 (2) What is the solution and how is it implemented?

SA-4 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*FedRAMP Assignment: at least the minimum requirement as defined in control CA-7*].

SA-4 (8) Additional FedRAMP Requirements and Guidance:

Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

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

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

SA-4 (9) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

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

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

SA-4 (10) Control Enhancement (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

SA-4 (10)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

SA-4 (10)	Control Summary Information
☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-4 (10) What is the solution and how is it implemented?

SA-5 Information System Documentation (L) (M)

The organization:

(a) Obtains administrator documentation for the information system, system component, or information system service that describes:

(5) Secure configuration, installation, and operation of the system, component, or service;
(6) Effective use and maintenance of security functions/mechanisms; and
(7) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

(b) Obtains user documentation for the information system, system component, or information system service that describes:

(8) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
(9) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
(10)User responsibilities in maintaining the security of the system, component, or service;

(mm) 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;

(nn) Protects documentation as required, in accordance with the risk management strategy; and

(oo) Distributes documentation to [*Assignment: organization-defined personnel or roles)*].

SA-5	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-5 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

SA-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

SA-8	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

SA-8	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SA-9 External Information System Services (L) (M) (H)

The organization:

(a) 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;

(b) Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

(c) Employs [*FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored*] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide https://www.FedRAMP.gov/documents

Guidance: Independent Assessors should assess the risk associated with the use of external services. See the FedRAMP page under Key Cloud Service Provider (CSP) Documents>FedRAMP Authorization Boundary Guidance

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

SA-9 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

SA-9 (1) Control Enhancement (M) (H)

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].

SA-9 (1)	Control Summary Information
Responsible Role:	
Parameter SA-9(1)(b):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

SA-9 (1)	**Control Summary Information**
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-9 (1) What is the solution and how is it implemented?	
Part a	
Part b	

SA-9 (2) Control Enhancement (M) (H)

The organization requires providers of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] to identify the functions, ports, protocols, and other services required for the use of such services.

SA-9 (2)	**Control Summary Information**
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SA-9 (4) Control Enhancement (M) (H)

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] are consistent with and reflect organizational interests.

SA-9 (4)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SA-9 (5) Control Enhancement (M) (H)

The organization restricts the location of [*FedRAMP Selection: information processing, information data, AND information services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Additional FedRAMP Requirements and Guidance

Guidance: System services refer to FTP, Telnet, and TFTP, etc.

SA-9 (5)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-9 (5) What is the solution and how is it implemented?

SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

(a) Perform configuration management during system, component, or service [*FedRAMP Selection: development, implementation, AND operation*];

(b) Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];

(c) Implement only organization-approved changes to the system, component, or service;

(d) Document approved changes to the system, component, or service and the potential security impacts of such changes; and

(e) Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-10 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

SA-10 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

SA-10 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-10 (1) What is the solution and how is it implemented?

SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

(a) Create and implement a security assessment plan;

(b) Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];

(c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

(d) Implement a verifiable flaw remediation process; and

(e) Correct flaws identified during security testing/evaluation.

SA-11	Control Summary Information
Responsible Role:	
Parameter SA-11(b)-1:	
Parameter SA-11(b)-2:	
Implementation Status (check all that apply):	

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

SA-11 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

SA-11 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

SA-11 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

SA-11 (1)	Control Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SA-11 (2) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

SA-11 (2)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SA-11 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (8)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SA-11 (8) What is the solution and how is it implemented?

13.16. System and Communications Protection (SC)

SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

(pp) Reviews and updates the current:

(1) System and communications protection policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) System and communications protection procedures [*FedRAMP Assignment: at least annually*].

SC-1	Control Summary Information
Responsible Role:	
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	

SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

SC-2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

SC-2	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

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

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

SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

SC-5	Control Summary Information
Responsible Role: Network Security Manager	
Parameter SC-5-1: Application layer floods, Distributed Denial of Service Attacks, Unintended Denial of Service attacks.	
Parameter SC-5-2: Using Cloud service providers, limiting network broadcast, network traffic monitoring, looking for warning signs, server redundancy, high-level network security, response plan	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ✅ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-5 What is the solution and how is it implemented?
The organization has defined safeguards against Application layers floods, Distributed Denial of Service and Unintentional Denial of Service attacks. Boundary protection devices such as gateway, router, firewall and encrypted tunnels are used. The network traffic is in constant monitoring using SolarWinds Event Log Analyser and Security Event Manager. The servers are made redundant and Azure Web Application Firewall is employed as a WAF. The firewalls are updated whenever a new update is launched. App Trana is used for vulnerability scanners, a patching service, and DDoS protection. The service can absorb extreme volumetric attacks and is able to distinguish DDoS from genuine surges in traffic. It develops rules and alert conditions for the websites and detects SYN, ICMP, UDP floods, etc. The security team develops an incident response plan that ensures staff members respond promptly and effectively in case of a DoS. McAfee MVISION is used as an antivirus.

SC-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

SC-6	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-7 Boundary Protection (L) (M) (H)

The information system:

(a) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and

(b) Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

(c) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

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

SC-7 What is the solution and how is it implemented?	
Part a	For boundary protection, gateways, routers,firewalls, guards, network-based malicious code analysis and virtualization systems, and encrypted tunnels are implemented within the information system. Site 24x7 is used as a monitoring tool for client endpoints, networks, servers, applications, and the cloud. SolarWinds Event Log Analyzer and Security Event Manager is also used for monitoring the network traffic to and from external and internal boundaries of the system which includes servers, routers, gateways, subnetworks, internal networks, and all data and packet transfer from and to the database servers. The network security manager monitors these event logs daily.
Part b	The subnetworks are physically separated from the internal network as the internal network is made with wired connections over the premise. Thus the internal network and the internal system resources are separated from the DMZ. DMZ is used by contractors or interns who do not need access to high security data for their responsible roles. The subnetworks are hosted in different cloud environment and virtual machines completely separated from the internal network by hosting them in separate servers and the network traffic and data transfer in these subnetworks are also in constant monitoring by the security manager with the help of SolarWinds Event Log Analyzer and Security Event Manager. Azure Web application firewall is also used to protect the subnetworks and Site 24x7 is used to monitor the boundary traffic from routers, servers, gateways, etc.
Part c	The connections to external networks are made using gateways, routers, guards, and encrypted tunnels. The data is encrypted in transit from these devices using Azure data encryption. The IP table rules for the routers are updated bi weekly based on the event log about the network traffics and data transfers. Penetration testing is performed monthly on these external connections to detect vulnerabilities. Pulse secure is used for VPN connections for secured system access. The rules in the routers ensures authorized traffic to confidential databases which blocks unwanted traffic to these database servers. Firewall such as Azure Web Application Firewall is implemented in the servers. The

SC-7 What is the solution and how is it implemented?	
	traffic from external network and boundaries is also monitored using Site 24x7 and logged using SolarWinds Event Log Analyzer.

SC-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

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

SC-7 (3) What is the solution and how is it implemented?
The organisation will implement appropriately strong access controls for systems that use the information system. For internet-facing services, such as remote access solutions, we enable multi-factor authentication or other alternatively strong access controls. Organisation will have an internal access point that is accessed only by authorised employees. And for the other users, there will use a guest network. Monitoring of incoming and outgoing communications traffic is made easier by restricting the number of external network connections. When switching from older to newer technologies, it's crucial to limit the number of external network connections to the system. Organisation will identify, document, and classify the access point so that no external factor can hack the systems. This makes it easier to avoid cross-communication and ensures any vulnerability within a said service cause a domino effect on all of the services.

SC-7 (4) Control Enhancement (M)

The organization:

(a) Implements a managed interface for each external telecommunication service;

(qq) Establishes a traffic flow policy for each managed interface;

(rr) Protects the confidentiality and integrity of the information being transmitted across each interface;

(ss) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(tt) Reviews exceptions to the traffic flow policy [*FedRAMP Assignment: at least at least annually*] and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7 (4)	Control Summary Information
Responsible Role: Network Security Engineer	
Parameter SC-7(4)(e): Annually	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (4) What is the solution and how is it implemented?	
Part a	The organization has built a dashboard to manage and interact with the various telecommunication services operated by the organization. This dashboard acts as an interface hub, a one a to many page that allows the users/clients to interact with their desired service. Although, the services seem to be at a singular spot within the interface they are encapsulated enough to prevent cross connection and snooping, to achieve this the interface uses network detouring technology to avoid collateral risks or man in the middle attacks.
Part b	There has to be a decent investment of time and human resources to monitor the traffic within this interface as it depends on a network detauring back end that makes requests to multiple APIs at once. To ease this, we will be implementing python scripts that parses through the traffic logs of the various different services , notifying the engineer who is on call to check for traffic incidents and

SC-7 (4) What is the solution and how is it implemented?	
	notify the authorities accordingly.
Part c	All the data from the interfaces to the backend API of the said service is first encrypted using, NordLocker, an encryption service by Nord Corporation, this tool is ideal for encrypting interface data, meta data, API tokens, interface private keys and user tokens. This makes it easier to avoid cross communication and ensures any vulnerability with in a said service cause a domino effect on all of the services.
Part d	The traffic flow policies ensure that there is no unusual activity within the communication between the users and services, this is a lot easier as we are keeping track what user is accessing what service with respect to the said user's unique access token, which is procedurally generated every 60 days as the company respects and follows the principle of least privilege, this further streamlines the right users for the said service which enables our scripts to easily detect any anomalies. This further helps in maintaining the right amount of traffic through these services in order not to overload them.
Part e	The traffic policy contains DNS routing configuration information. Health checks for the endpoints are conducted by using probes through container orchestrators and load balancers. The policy contains Name (JailFromHome), version (1 in our case), version description (basic version), DNS type(CloudFront distribution - IP4 format),Connect to (Failover rule,geolocation rule,latency rule, geoproximity rule, Multi value answer rule, weighted rule), value type(CloudFront distribution,ELB load balancer,S3 website endpoint). Based on the option chosen for each application, the exceptions are removed.

SC-7 (5) Control Enhancement (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

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

SC-7 (5) What is the solution and how is it implemented?
An organization's privacy framework will include a firewall that by default will block all network connections. The traffic will be screened, and will initially be by default rejected. On the firewall, the network engineer will create an Access lists that only permits vital traffic to enter the network. As a result, both inbound and outbound network communications traffic fall under this definition of allowing by exception. With a deny-all, permit-by-exception network communications traffic policy, only authorized and necessary system connections are permitted. It also applies to a system that is connected to an external system: deny by default, allow by exception.

SC-7 (7) Control Enhancement (M) (H)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

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

SC-7 (7) What is the solution and how is it implemented?
To mitigate the risk of split tunneling, the remote workstations used by the third parties are verified using Netsh. For internal employees and contractors, they have to comply with Acceptable Use Policy (AUP) to use the equipment according to acceptable terms. Employers are trained to use equipment in the Employee Equipment Training (EET) program, which imparts training on acceptable and non-acceptable usage of the equipment (workstations and remote connections). VPN agents like Sentient Digital is used which checks the health of the device and checks its compliance. The Health checks include checking Operating systems (MacOS,Windows, Linux-based on application), anti-virus software (McAfee is up to date and is latest in version). Firewalls - SonicWall is installed in front of the VPN traffic.

SC-7 (8) Control Enhancement (M) (H)

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

SC-7 (8)	Control Summary Information
Responsible Role: Network Security Engineer	
Parameter SC-7(8)-1: DNS resolver	
Parameter SC-7(8)-2: TLD name server	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (8) What is the solution and how is it implemented?
The personnel of the Homeland Security type in the website they want to visit to access parolee's data, that is stored in AWS cloud. The request is routed to DNS resolver managed by Homeland Security's ISP. The ISP forwards it to DNS root name server. It is forwarded to one of the TLD name server for .org domains. The name server for the .org responds to the request of four Route 53 name servers associated with website domain. The DNS resolver stores the name servers so that the next time if someone needs it, it is already available and need not have to go through out the process again.The Route 53 name server looks in the website domain to get hosted zone, and hence the traffic is routed.

SC-7 (12) Control Enhancement (M)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

SC-7 (12)	Control Summary Information
Responsible Role: Network Security Engineer	
Parameter SC-7(12)-1: Host based firewalls	
Parameter SC-7(12)-2: Workstations	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ✅ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (12) What is the solution and how is it implemented?
Host based firewall is installed and configured. The system is secured with good passwords and default ones are changed. Operating systems patches are installed and upgraded. Hardware firmware patches are also installed and configured. Logs on the devices are monitored. Services and devices that are no longer needed or used are disabled. Insecure services such as telnet, rsk or rlogin are replaced with more secure alternatives such as ssh. The services which cannot be disabled are restricted in accesses. The test backups are frequently made,updated in consistent manner.

SC-7 (13) Control Enhancement (M)

The organization isolates [*FedRAMP Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7 (13) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

SC-7 (13)	Control Summary Information
Responsible Role: Network Security Engineer	
Parameter SC-7(13): Logically separate subnets using Private Vlan and Azuru	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ✅ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (13) What is the solution and how is it implemented?
In order to help separate the network, an organization's network has implemented a method called The communication between the VLANs will be divided by assigning each sector to a different VLAN. The organization's whole security setup will be housed in a separate network that can only be accessed by approved staff members. Subnetworks are additionally protected by Azure Web application firewall, and Site 24x7 monitors border traffic from routers, servers, gateways, and other devices. In order to keep intruders from learning about the analysis and forensics methods used by businesses using FDA, it is important to physically isolate computer network defenses from crucial operational processing networks using controlled interfaces. Further the organisation has implemented the Intrusion detection systems (IDS) and intrusion prevention systems (IPS) which constantly watch network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators.

SC-7 (18) Control Enhancement (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

SC-7 (18)	Control Summary Information
Responsible Role: Network Security Engineer	
Implementation Status (check all that apply): ✅ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

SC-7 (18)	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ✅ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (18) What is the solution and how is it implemented?
To stay on top of cyber threats, spot anomalies and incidents that have a negative impact on IT and data, and lessen the impact of, deal with, and recover from incidents, a rigorous framework must be established. A dual-home connection using the technology HSRP, is used by organizations to ensure that they can continue operating even if something goes wrong with one connection. There will to connection from the IPS. An incident response team, trained to respond in failure scenarios, is present in the organization. To make sure that its infrastructure is well protected, the company conducted pentration testing. Boundary protection device malfunctions cannot result in or cause information from outside the devices to enter them, nor can they allow illegal information releases. All the routers, firewalls, and application gateways that reside on protected subnetworks are secured. Network traffic is also observed using Security Event Manager and SolarWinds Event Log Analyzer.

SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [*FedRAMP Assignment: confidentiality AND integrity*] of transmitted information.

SC-8	Control Summary Information
Responsible Role:	
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)	

SC-8	Control Summary Information
☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-8 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to [*FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information*] during transmission unless otherwise protected by [*FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)*].

SC-8 (1)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-10 Network Disconnect (M)

The information system terminates the network connection associated with a communications session at the end of the session or after [*FedRAMP Assignment: no longer than thirty (30) minutes for RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions*] of inactivity.

SC-10	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

SC-12	Control Summary Information
Responsible Role:	

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

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

SC-12 (2) Control Enhancement (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [*FedRAMP Selection: NIST FIPS-compliant*] key management technology and processes.

SC-12 (2)	Control Summary Information
Responsible Role:	
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)	

SC-12 (2)	Control Summary Information
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-12 (3) Control Enhancement (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].

SC-12 (3)	Control Summary Information
Responsible Role:	
Parameter SC-12 (3):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-12 (3) What is the solution and how is it implemented?

SC-13 Use of Cryptography (L) (M) (H)

The information system implements [*FedRAMP Assignment: FIPS-validated or NSA-approved cryptography]* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-13	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-15 Collaborative Computing Devices (M) (H)

The information system:

(a) Prohibits remote activation of collaborative computing devices with the following exceptions:[*FedRAMP Assignment: no exceptions*]; and

(b) Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

SC-15	Control Summary Information
Responsible Role:	
Parameter SC-15(a):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-15 What is the solution and how is it implemented?	
Part a	
Part b	

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

SC-15 Req.	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)	

SC-15 Req.	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-15 What is the solution and how is it implemented?	
Req. 1	

SC-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates from an approved service provider.

SC-17	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-17 What is the solution and how is it implemented?

SC-18 Mobile Code (M) (H)

The organization:

(a) Defines acceptable and unacceptable mobile code and mobile code technologies;

(b) Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

(c) Authorizes, monitors, and controls the use of mobile code within the information system.

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-18 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

SC-19 Voice Over Internet Protocol (M) (H)

The organization:

(a) Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

(b) Authorizes, monitors, and controls the use of VoIP within the information system.

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

(a) 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

(uu) 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	

SC-20	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-21 What is the solution and how is it implemented?

SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

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

SC-22 What is the solution and how is it implemented?

SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

SC-23	Control Summary Information
Responsible Role:	

SC-23	Control Summary Information
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-23 What is the solution and how is it implemented?

SC-28 Protection of Information at Rest (M) (H)

The information system protects the [*FedRAMP Selection: confidentiality AND integrity]*] of [*Assignment: organization-defined information at rest*].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

SC-28	Control Summary Information
Responsible Role:	
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	

SC-28	Control Summary Information
☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-28 What is the solution and how is it implemented?

SC-28 (1) Control Enhancement (M)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*]

SC-28 (1)	Control Summary Information
Responsible Role:	
Parameter SC-28(1)-1:	
Parameter SC-28(1)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-28 (1) What is the solution and how is it implemented?

SC-39 Process Isolation (L) (M) (H)

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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-39 What is the solution and how is it implemented?

13.17. System and Information Integrity (SI)

SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

(a) Reviews and updates the current:

(1) System and information integrity policy [*FedRAMP Assignment: at least every three*

(3) years]; and

(3) System and information integrity procedures [*FedRAMP Assignment: at least 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	

SI-2 Flaw Remediation (L) (M) (H)

The organization:

(a) Identifies, reports, and corrects information system flaws;

(a) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

(b) Installs security-relevant software and firmware updates within [*FedRAMP Assignment: thirty 30 days of release of updates*] of the release of the updates; and

(c) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [*FedRAMP Assignment: at least monthly*] to determine the state of information system components with regard to flaw remediation.

SI-2 (2)	**Control Summary Information**
Responsible Role:	
Parameter SI-2 (2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

SI-2 (2)	Control Summary Information
☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-2 (3) Control Enhancement (M) (H)

The organization:

(a) Measures the time between flaw identification and flaw remediation; and

(a) Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

SI-2 (3)	Control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-2 (3) What is the solution and how is it implemented?	
Part a	
Part b	

SI-3 Malicious Code Protection (L) (M)

The organization:

(a) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

(a) Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

(b) Configures malicious code protection mechanisms to:

(4) 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

(5) [*FedRAMP Assignment: to include alerting administrator or defined security personnel*] in response to malicious code detection; and

(c) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-3 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

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

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

SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

SI-3 (2)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply):	

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

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

SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

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

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

SI-4 Information System Monitoring (L) (M) (H)

The organization:

(a) Monitors the information system to detect:

(6) Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

(7) Unauthorized local, network, and remote connections;

(d) Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

(e) 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;

(f) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

(g) 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;

(h) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

(vv) Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed; [Assignment: organization-defined frequency*]].

SI-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

SI-4	Control Summary Information
Responsible Role:	
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	

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

SI-4 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	

SI-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

SI-4 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

SI-4 (1)	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

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

SI-4 (2) What is the solution and how is it implemented?

SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [*FedRAMP Assignment: continuously]* for unusual or unauthorized activities or conditions.

SI-4 (4)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-4 (5) Control Enhancement (M) (H)

The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

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

Guidance: In accordance with the incident response plan.

SI-4 (5)	Control Summary Information
Responsible Role:	
Parameter SI-4(5)-1:	
Parameter SI-4(5)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

SI-4 (5)	Control Summary Information
☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

SI-4 (14)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-4 (14) What is the solution and how is it implemented?

SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

SI-4 (16)	**Control Summary Information**
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-4 (16) What is the solution and how is it implemented?

SI-4 (23) Control Enhancement (M) (H)

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

SI-4 (23)	**Control Summary Information**
Responsible Role:	
Parameter SI-4(23)-1:	
Parameter SI-4(23)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

SI-4 (23)	**Control Summary Information**
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-4 (23) What is the solution and how is it implemented?

SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

(a) Receives information system security alerts, advisories, and directives from [*FedRAMP Assignment: to include US-CERT*] on an ongoing basis;

(i) Generates internal security alerts, advisories, and directives as deemed necessary;

(j) Disseminates security alerts, advisories, and directives to [*FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities*]; and

(k) 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	

SI-5	Control Summary Information
☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-5 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

SI-6 Security Functionality Verification (M) (H)

The information system:

(a) Verifies the correct operation of [*Assignment: organization-defined security functions*];

(b) Performs this verification [*FedRAMP Assignment: to include upon system startup and/or restart at least monthly*];

(c) Notifies [*FedRAMP Assignment: to include system administrators and security personnel*] of failed security verification tests; and

(d) [*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	

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

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

SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

SI-7	Control Summary Information
Responsible Role:	
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)	

SI-7	Control Summary Information
☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events*]; [*FedRAMP Assignment: at least monthly*]].

SI-7 (1)	Control Summary Information
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

SI-7 (7)	**Control Summary Information**
Responsible Role:	
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 FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-7 (7) What is the solution and how is it implemented?

SI-8 Spam Protection (M) (H)

The organization:

(a) Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

(b) Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

SI-8	**Control Summary Information**
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

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

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

SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

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

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

SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

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

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

SI-10 Information Input Validation (M) (H)

The information system checks the validity of [*Assignment: organization-defined information inputs*].

SI-10	Control Summary Information
Responsible Role:	
Parameter SI-10:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

SI-10	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-11 Error Handling (M) (H)

The information system:

(a) Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

(b) Reveals error messages only to [*Assignment: organization-defined personnel or roles*].

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)	

SI-11	Control Summary Information
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

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

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

SI-16 Memory Protection (M) (H)

The information system implements [*Assignment: organization-defined fail-safe procedures*] to protect its memory from unauthorized code execution.

SI-16	Control Summary Information
Responsible Role:	
Parameter SI-16-1:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SI-16 What is the solution and how is it implemented?

14. Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

SYSTEMS SECURITY PLAN ATTACHMENTS

Instruction: Attach any documents that are referred to in the Information System Name (Enter Information System Abbreviation) System Security Plan. Documents and attachments should, provide the title, version and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.

Delete this and all other instructions from your final version of this document.

15. Attachments

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. Attachment File Naming Convention to differentiate between them using the "xx" portion of the File Name. *Example* Enter Information System Abbreviation *A1 ISPP xx v1.0*. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. Attachment File Naming Convention. (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Names of Provided Attachments

Attachment	File Name	File Extension
Information Security Policies and Procedures	Enter Information System Abbreviation A1 ISPP xx v1.0	. enter extension
User Guide	Enter Information System Abbreviation A2 UG v1.0	. enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA If needed)	Enter Information System Abbreviation A4 PIA v1.0	. enter extension
Rules of Behavior	Enter Information System Abbreviation A5 ROB v1.0	. enter extension
Information System Contingency Plan	Enter Information System Abbreviation A6 ISCP v1.0	. enter extension
Configuration Management Plan	Enter Information System Abbreviation A7 CMP v1.0	. enter extension

Attachment	File Name	File Extension
Incident Response Plan	Enter Information System Abbreviation A8 IRP v1.0	. enter extension
CIS Workbook	Enter Information System Abbreviation A9 CIS Workbook v1.0	. enter extension
FIPS 199	Included in Section 15	
Inventory	Enter Information System Abbreviation A13 INV v1.0	. enter extension

Attachment 1 Information Security Policies and Procedures

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

Attachment 2 User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

Attachment 3 Digital Identity Worksheet

This Attachment Section has been revised to include the Digital Identity template. Therefore, a separate attachment is not needed. Delete this note and all other instructions from your final version of this document.

The Digital Identity section explains the objective for selecting the appropriate Digital Identity levels for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, Digital Identity Guidelines.

Introduction and Purpose

This document provides guidance on digital identity services (Digital Identity, which is the process of establishing confidence in user identities electronically presented to an information system). Authentication focuses on the identity proofing process (IAL), the authentication process (AAL), and the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) (FAL). NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

NIST SP 800-63-3 can be found at the following URL: NIST SP 800-63-3

Information System Name/Title

This Digital Identity Plan provides an overview of the security requirements for the (Enter Information System Abbreviation) in accordance with NIST SP 800-63-3.

Table 15-2. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
Enter FedRAMP Application Number.		Enter Information System Abbreviation

Digital Identity Level Definitions

NIST SP 800-63-3 defines three levels in each of the components of identity assurance to categorize a federal information system's Digital Identity posture. NIST SP 800-63-3 defines the Digital Identity levels as:

- IAL – refers to the identity proofing process.

- AAL – refers to the authentication process.
- FAL – refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

FedRAMP maps its system categorization levels to NIST 800-63-3's levels as shown in Table 15-3:

Table 15-3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels

FedRAMP System Categorization	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
High	IAL3: In-person, or supervised remote identity proofing	AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques	FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Moderate	IAL2: In-person or remote, potentially involving a "trusted referee"	AAL2: Multi-factor required, using approved cryptographic techniques	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Low	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider
FedRAMP Tailored LI-SaaS	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider

Selecting the appropriate Digital Identity level for a system enables the system owner to determine the right system authentication technology solution for the selected Digital Identity levels. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63-3.

Review Maximum Potential Impact Levels

CSP Name has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user's asserted identity. CSP Name has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15-4 Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15-4. Potential Impacts for Assurance Levels

	Assurance Level Impact Profile		
Potential Impact Categories	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Mod	High
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

Digital Identity Level Selection

Instruction: Select the lowest level that will cover all potential impact identified from Table 15-4 Potential Impacts for Assurance Levels.

Delete this instruction from your final version of this document.

The CSP Name has identified that they support the Digital Identity Level that has been selected for the <Information System Name> as noted in Table 15-5 Digital Identity Level. The selected Digital Identity Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the Digital Identity mechanisms are provided in the System Security Plan under control IA-2.

Table 15-5. Digital Identity Level

Digital Identity Level	Maximum Impact Profile	Selection
Level 1: AAL1, IAL1, FAL1	Low	☐
Level 2: AAL2, IAL2, FAL2	Moderate	☐
Level 3: AAL3, IAL3, FAL3	High	☐

Attachment 4 **PTA / PIA**

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in ATTACHMENT 12 – FedRAMP Laws and Regulations.

Privacy Overview and Point of Contact (POC)

The Table 15-6 - Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

Table 15-6. - Information System Name; Privacy POC

Name	Click here to enter text.
Title	Click here to enter text.
CSP / Organization	Click here to enter text.
Address	Click here to enter text.
Phone Number	Click here to enter text.
Email Address	Click here to enter text.

Applicable Laws and Regulations

The FedRAMP Laws and Regulations may be found on: Templates. A summary of FedRAMP Laws and Regulations is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations.

Table 12-1 Information System Name Laws and Regulations include additional laws and regulations that are specific to <Information System Name>. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 15-7. <Information System Name> Laws and Regulations

Identification Number	Title	Date	Link
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

Applicable Standards and Guidance

The FedRAMP Standards and Guidance may be found on: Templates. The FedRAMP Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the FedRAMP website.

Table 12-2 Information System Name Standards and Guidance includes any additional standards and guidance that are specific to <Information System Name>. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table 15-8. <Information System Name> Standards and Guidance

Identification Number	Title	Date	Link
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social Security numbers
- Passport numbers
- Driver's license numbers
- Biometric information
- DNA information

- Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

Privacy Threshold Analysis

CSP Name performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the <Information System Name> (Enter Information System Abbreviation) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by CSP Name can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

Qualifying Questions

Select One	Does the ISA collect, maintain, or share PII in any identifiable form?
Select One	Does the ISA collect, maintain, or share PII information from or about the public?
Select One	Has a Privacy Impact Assessment ever been performed for the ISA?
Select One	Is there a Privacy Act System of Records Notice (SORN) for this ISA system? If yes; the SORN identifier and name is: Enter SORN ID/Name.

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

Designation

Check one.

□	A Privacy Sensitive System
□	Not a Privacy Sensitive System (in its current version)

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: Templates.

Attachment 5 Rules of Behavior

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a CSP to implement rules of behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: Templates.

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The CSP should modify each of these two sets to define the rules of behavior necessary to secure their system.

Attachment 6 Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: Templates.

The Information System Contingency Plan Template is provided for CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

Attachment 7 Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

Attachment 8 INCIDENT RESPONSE PLAN

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

Attachment 9 CIS Workbook

All Authorization Packages must include Control Implementation Summary (CIS) Workbook attachment, which will be reviewed for quality.

The Template can be found on the following FedRAMP website page: Templates.

Attachment 10 FIPS 199

This Attachment Section has been revised to include the FIPS 199 Template. Therefore, a separate PTA attachment is not needed. Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

The FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

Introduction and Purpose

This section is intended to be used by service providers who are applying for an Authorization through the U.S. federal government FedRAMP program.

The Federal Information Processing Standard 199 (FIPS 199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The FIPS199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment.

The purpose of the FIPS199 Categorization report is for the CSP to assess and complete the categorization of their cloud environment, to provide the categorization to the System Owner/Certifier and the FedRAMP Joint Authorization Board (JAB) and in helping them to make a determination of the CSP's ability to host systems at that level. The completed security categorization report will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

System Description

The <Information System Name> system has been determined to have a security categorization of Choose level.

Instruction: Insert a brief high-level description of the system, the system environment and the purpose of the system. The description should be consistent with the description found in the System Security Plan (SSP).
Delete this instruction from your final version of this document.

Methodology

Instruction: The CSP should review the NIST Special Publication 800-60 Volume 2 Revision 1 Appendix C Management and Support Information and Information System Impact Levels and Appendix D Impact Determination for Mission-Based Information and Information Systems to assess the recommended impact level for each of the information types. For more information, the CSP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the CSP should fill out Table 2-1 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1.
Delete this instruction from your final version of this document.

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 199 analysis represents the information type and sensitivity levels of the CSP's cloud service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 Categorization report analysis for their own data hosted on the CSP's cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

Instruction: In the first three columns, put the NIST SP-60 V2 R1 recommended impact level. In the next three columns, put in the CSP determined recommended impact level. If the CSP determined recommended impact level does not match the level recommended by NIST, put in an explanation in the last column as to why this decision was made.
Delete this instruction from your final version of this document.

The Table 2-1 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table 15-9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

Information Type	NIST SP 800-60 V2 R1 Recommended Confidentiality Impact Level	NIST SP 800-60 V2 R1 Recommended Integrity Impact Level	NIST SP 800-60 V2 R1 Recommended Availability Impact Level	CSP Selected Confidentiality Impact Level	CSP Selected Integrity Impact Level	CSP Selected Availability Impact Level	Statement for Impact Adjustment Justification
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.

Attachment 11 Separation of Duties Matrix

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

ATTACHMENT 11 - Separation of Duties Matrix is referenced in the following controls.

AC-5 Separation of Duties (M) (H) Additional FedRAMP Requirements and Guidance

Attachment 12 FedRAMP Laws and Regulations

The Table 15-8 FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance are referenced.

Table 15-10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance

Phase		Document Title	
Document Phase		SSP	System Security Plan
	SSP Attachment 4	PTA/PIA	Privacy Threshold Analysis and Privacy Impact Assessment
	SSP Attachment 6	ISCP	Information System Contingency Plan
	SSP Attachment 10	FIPS 199	FIPS 199 Categorization
Assess Phase		SAP	Security Assessment Plan
Authorize Phase		SAR	Security Assessment Report

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: Templates.

Note: All NIST Computer Security Publications can be found at the following URL: http://csrc.nist.gov/publications/PubsSPs.html

Attachment 13 FedRAMP Inventory Workbook

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

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