FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

Hope Health Care Information System

Version 1

2020.3.7

FedRAMP

CONTROLLED UNCLASSIFIED INFORMATION

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	<Enter Company/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
6/20/2016	Original publication
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 Section 10 and Attachment 13 Removed chapter numbers from Attachments Removed 3 questions from Sec 2.3 E-Authentication Determination
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

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
3/4/2020	First vision	1	Team 1
<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 (HHCIS) 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. Health Care Information System

Unique Identifier	Information System Name	Information System Abbreviation
<Enter FedRAMP Application Number>	Hope Health Care Information System	HHCIS

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:	High (H)

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.

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
Access to Care	D.14.1	Low(L)	Moderate(L)	Low(L)
Population Health Management and Consumer Safety	D.14.2	Low(L)	Moderate(M)	Low(L)
Health Care Administration	D.14.3	Low (L)	Moderate (M)	Low (L)
Health Care Delivery Services	D.14.4	Low (L)	High (H)	Low (L)
<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	Low (L)
Integrity	High (H)
Availability	Low (L)

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	High (H)

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 Level 3: AAL3, IAL3, FAL3

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>.

Information System Owner Information	
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4. AUTHORIZING OFFICIALS

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>.
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.

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.

Question (Yes/No)	Conclusion
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.

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.

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. cAdd 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

Hope Health Care Information System is a general information system for small and medium-sized hospitals. It covers the main management functions of hospitals and the main links of patients in hospitals.

HHCIS integrates the management of the hospital and the business of each department into the information system. In the aspect of system function, it realizes the unified management of drug management, outpatient management, inpatient and ward management, medical file management, medical device management, financial management, human resource management and other modules.

This system can bring convenient and fast services to patients, promote standardized management of hospitals, and greatly reduce medical errors.

9.2. Information System Components and Boundaries

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

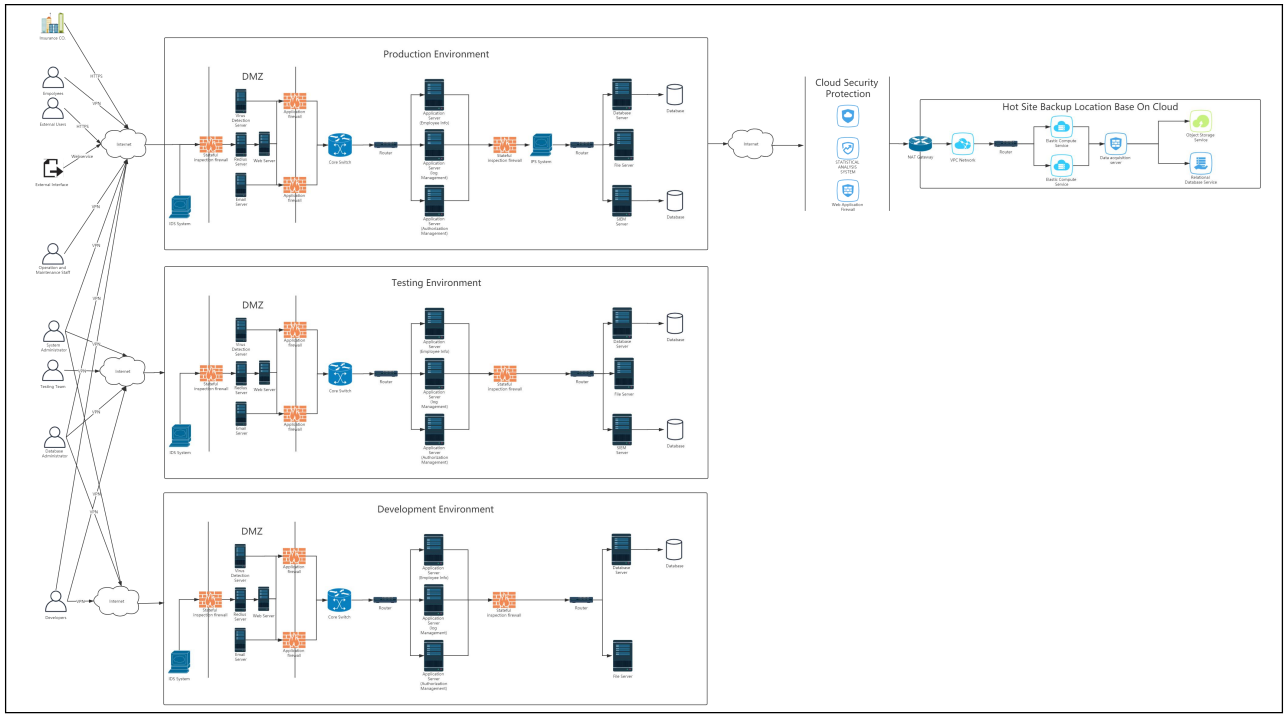

Figure 9- 1. Authorization Boundary Diagram

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.

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
System Administrator	Internal	P	High-Risk	Full administrative access (root)	Add/remove users and hardware, install and configure

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
					software, OS updates, patches and hotfixes, perform backups
Database Administrator	Internal	NP	Severe	Portal administration	Monitor the warning log of the database, and make regular backup and deletion; password management; authorization ; assign resources
Web Administrator	Internal	NP	Moderate	Portal administration	Design, develop, operate and maintain the webpages
Network Administrator	Internal	NP	Moderate	Portal administration	Network architecture design, installation and configuration
Firewall Administrator	Internal	NP	Moderate	Portal administration	Plan and deploy the firewall, formulate policies, and configure and test rules; monitor the status of the firewall and perform audit analysis on the firewall logs.
Client Administrator	Internal	NP	Moderate	Portal administration	Add/remote client users. Create, modify and delete client applications
Test Team	Internal	NP	Moderate	Portal administration	Interface test, security test, function test, installation test
Development Team	Internal	NP	Moderate	Access to development environment	System function development
Operation and maintenance staff	Internal	NP	Moderate	Portal administration	Perform daily operation and maintenance of the system, check the backup, update version, etc
Hospital Staff	External	NP	N/A	Portal administration	Input, query and manage patient information; hospital

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
					resource and medical document query; salary payment; human resource management; do office work
Patient	External	NP	N/A	Portal access to system	Access to the hospital website; for inquiry; make an appointment online
Insurance Company	External	NP	N/A	Portal access to system	If the patient has bought medical insurance, the insurance company can obtain the patient's medical information from the system and make Insurance compensation..

There are currently 200 internal personnel and 5000 external personnel. Within one year, it is anticipated that there will be 300 internal personnel and 7000 external personnel.

9.4. Network Architecture

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.

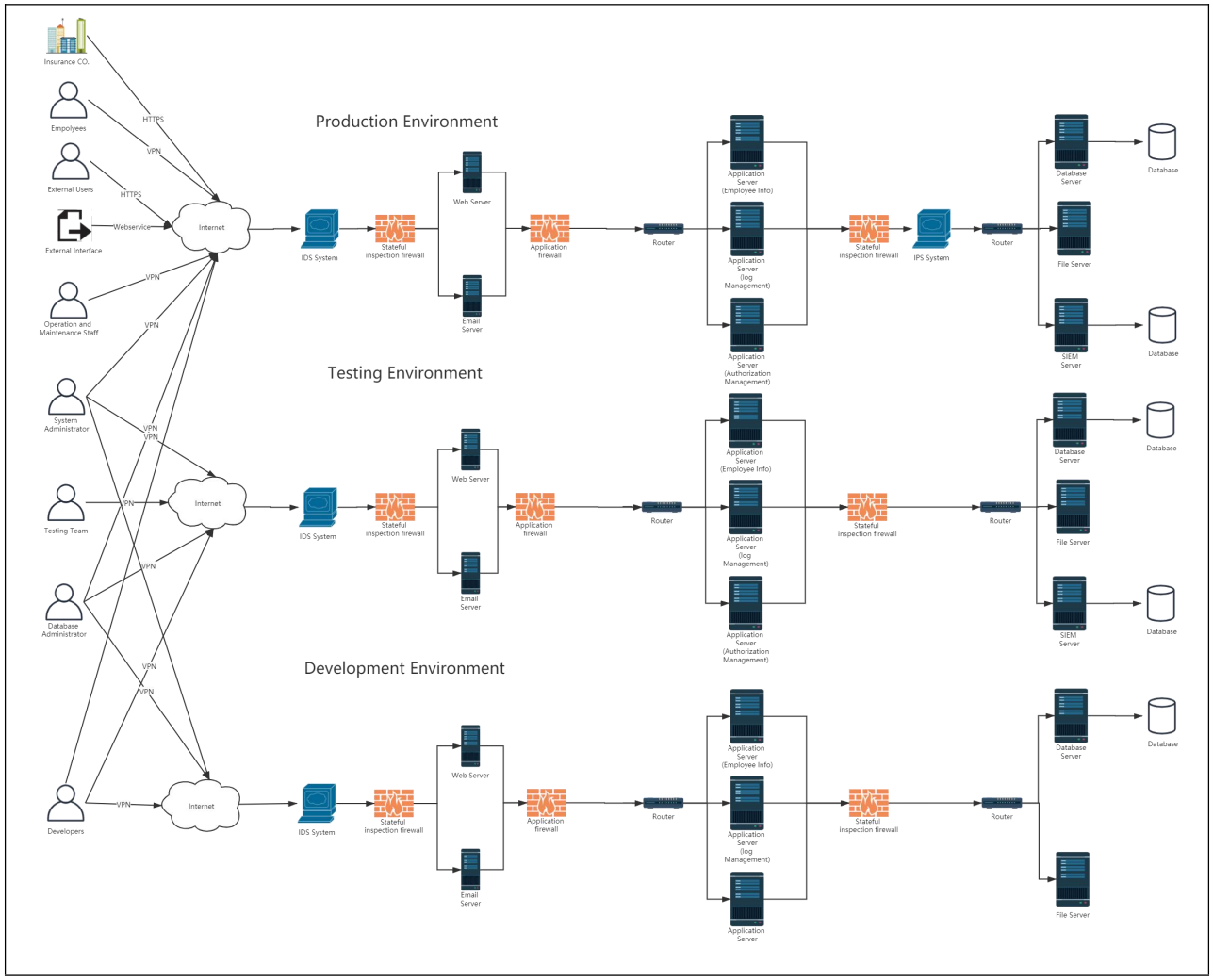

Figure 9- 2. Network Diagram

10. SYSTEM ENVIRONMENT AND INVENTORY

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

10.1. Data Flow

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

Through the data flow chart, we can learn that in the production environment, all external users can send access requests to HHCIS through the Internet and internal employees (including managers, administrators, etc.) through VPN. These information is first received by IDS, which can filter and help detect whether these requests are threatening. The allowed request will be sent to the web server. If it is an HTTPS security request, it will provide the web browsing service provided by the system. When users use some functions (such as login, registration, query, etc.) in the web page, these requests will be sent to the first router, which can act as a data bridge, change the path and optimize the measurement by using different information from different sources through the algorithm, and confirm whether these users are authorized enough. Next, different application servers will receive request information using different functions, and provide a simple and manageable access mechanism to system resources for web applications by calling different methods. It is worth noting that we have established an application server to handle log and authorization management in the environment. They can help the administrator handle some security events to ensure the system's CIA (confidentiality, integrity, availability). When the application server needs to read and write data (such as add, delete, change, etc.), it will send read and write requests to the data server, file server and Siem server. These requests are first filtered by IPS. As a computer network security device that monitors the network or network device's network data transmission behavior, IPS can immediately interrupt, adjust or isolate some abnormal or harmful network data transmission behavior. When the request is allowed, the data server, file server and Siem server will be requested and connect the file or allow database, finally forming the functions required by users.
In addition, although the complete data flow is similar in the test environment and the development environment, it needs to meet the availability of functions in the development environment and the security access control to meet all needs in the test environment, so as to ensure that the data flow in the production environment has the smallest security threat.

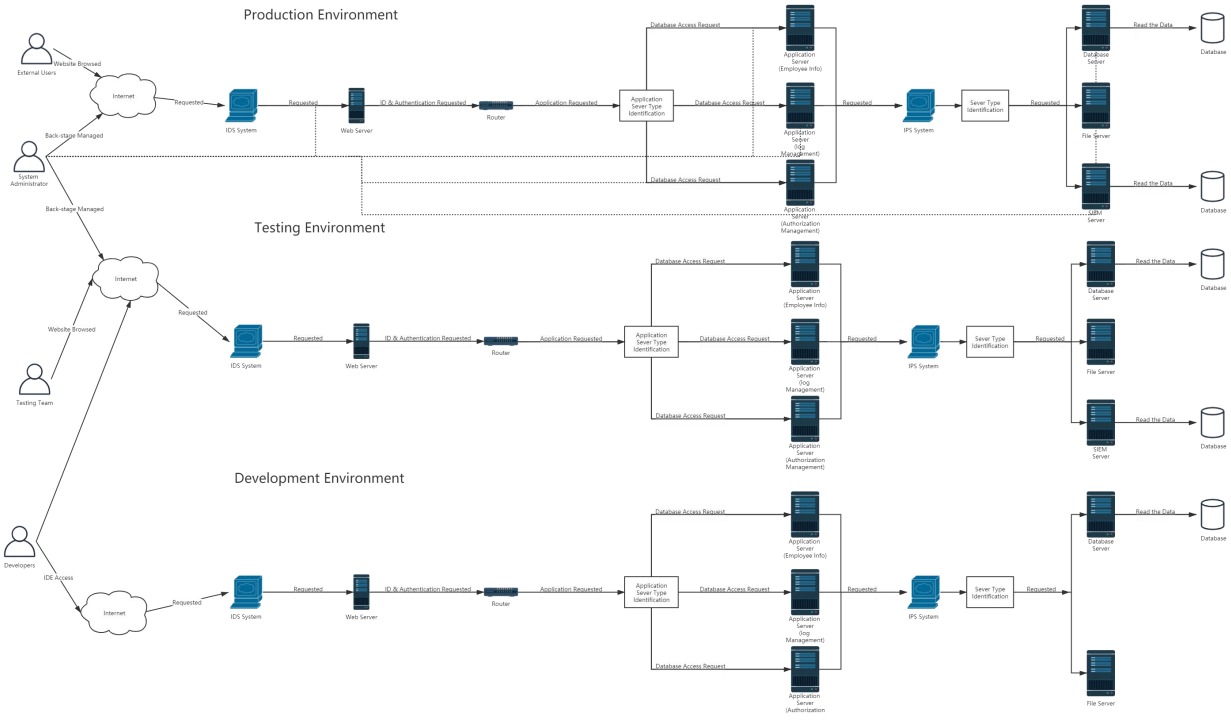

Figure 10- 1. Data Flow Diagram

10.2. Ports, Protocols and Services

The 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

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>	Backup System Company	Young 111-111-1111	VPN	Incoming and outgoing	All kinds of data	<Port/Circuit Numbers>
<SP IP Address/Interface>	Security Monitoring System Company	Jane 222-222-2222	SSL	Outgoing	All kinds of data	<Port/Circuit Numbers>
<SP IP Address/Interface>	Insurance Company	Kevin 333-333-3333	HTTPS	Outgoing	Patient information	<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/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

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
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

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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
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				

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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
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)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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)
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

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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 Documentation	SA-5	SA-5	SA-5
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

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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)
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.

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 (H)

The organization:

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

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

associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually]*; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1	Control Summary Information
Responsible Role: CIO	
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	
Part b2	

AC-2 Account Management (H)

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: monthly for privileged accessed, every six (6) months for non-privileged access*]; 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: System Administrator	
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)	

AC-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 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 (H)

The information system automatically [*FedRAMP Selection: disables*] temporary and emergency accounts after [*FedRAMP Assignment: 24 hours from last use*].

AC-2 (2)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-2(2)1:	
Parameter AC-2(2)2:	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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 (H)

The information system automatically disables inactive accounts after [*FedRAMP Assignment: thirty-five (35) 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 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: System Administrator	
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 (H)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*FedRAMP Assignment: organization and/or service provider system owner*].

AC-2 (4)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-2(4):	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned	

AC-2 (4)	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	

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

AC-2 (5) CONTROL ENHANCEMENT (H)

The organization requires that users log out when [*FedRAMP Assignment: inactivity is anticipated to exceed fifteen (15) minutes*].

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: System Administrator	
Parameter AC-2(5):	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility)	

AC-2 (5)	Control Summary Information
☐ 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 (H)

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;

(b) Monitors privileged role assignments; and

(c) Takes [*FedRAMP Assignment: disables//revokes access within an organization-specified timeframe*] when privileged role assignments are no longer appropriate.

AC-2 (7)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-2(7)(c):	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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	

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

AC-2 (9) CONTROL ENHANCEMENT (H)

The organization only permits the use of shared/group accounts that meet [*FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary*].

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

AC-2 (9)	Control Summary Information
Responsible Role: System Administrator	
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?

(a) Reports atypical usage of information system accounts to [*FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization*].

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

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

AC-2 (13) CONTROL ENHANCEMENT (H)

The organization disables accounts of users posing a significant risk within [*FedRAMP Assignment: one (1) hour*] of discovery of the risk.

AC-2 (13)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-2 (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	

AC-2 (13) What is the solution and how is it implemented?

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: CIO	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AC-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	

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

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

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

AC-4 (8) CONTROL ENHANCEMENT (H)

The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*].

AC-4 (8)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-4 (8)-1:	
Parameter AC-4 (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	

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

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: System Administrator	
Parameter AC-4 (21)-1:	
Parameter AC-4 (21)-2:	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

AC-6 (1) CONTROL ENHANCEMENT (H)

The organization explicitly authorizes access to [*FedRAMP Assignment: all functions not publicly accessible and all security-relevant information not publicly available*].

AC-6 (1)	Control Summary Information

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

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

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: System Administrator	
Parameter AC-6 (2)	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented	

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

AC-6 (3) CONTROL ENHANCEMENT (H)

The organization authorizes network access to [*FedRAMP Assignment: all privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

AC-6 (3)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-6 (3)-1:	
Parameter AC-6 (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)	

AC-6 (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	

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

AC 6 (5) CONTROL ENHANCEMENT (M) (H)

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

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

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

AC-6 (7) CONTROL ENHANCEMENT (H)

The organization:

(a) Reviews [*FedRAMP Assignment: at a minimum, annually*] the privileges assigned to [*FedRAMP Assignment: all users with privileges*] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

AC-6 (7)	Control Summary Information
Responsible Role: Auditor	
Parameter AC-6 (7)(a)-1:	
Parameter AC-6 (7)(b)-2:	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-6 (7) What is the solution and how is it implemented?	
Part a	
Part b	

AC-6 (8) CONTROL ENHANCEMENT (H)

The information system prevents [*FedRAMP Assignment: any software except software explicitly documented*] from executing at higher privilege levels than users executing the software.

AC-6 (8)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-6 (8):	

AC-6 (8)	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-6 (8) What is the solution and how is it implemented?

AC-6 (9) CONTROL ENHANCEMENT (M) (H)

The information system audits the execution of privileged functions.

AC-6 (9)	Control Summary Information
Responsible Role: 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)	

AC-6 (9)	Control Summary Information
☐ 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?

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: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

AC-7 Unsuccessful Login Attempts (H)

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

(b) Automatically [*Selection: locks the account/node for a* [*FedRAMP Assignment: minimum of three (3) hours or until unlocked by an administrator*]; *delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

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

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

AC-7 (2) CONTROL ENHANCEMENT (H)

The information system purges/wipes information from [*FedRAMP Assignment: mobile devices as defined by organization policy*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after [*FedRAMP Assignment: three (3)*] consecutive, unsuccessful device logon attempts.

AC-7 (2)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-7(2)-1:	
Parameter AC-7(2)-2:	
Parameter AC-7(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-7 (2) What is the solution and how is it implemented?

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;

(b) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

(c) For publicly accessible systems:

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

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/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: System Administrator	
Parameter AC-8(a):	
Parameter AC-8(c)-1:	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AC-8	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-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: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented	

AC-8 Req.	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-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: System Administrator	
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	

AC-10	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-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

(b) Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11	Control Summary Information
Responsible Role: System Administrator	
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: System Administrator	

AC-12	Control Summary Information
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) ☐ 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-12 (1) CONTROL ENHANCEMENT (H)

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*]; and

(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

AC-8 Additional FedRAMP Requirements and Guidance:

Guidance: Testing for logout functionality (OTG-SESS-006) https://www.owasp.org/index.php/Testing_for_logout_functionality_%28OTG-SESS-006%29

AC-12 (1)	Control Summary Information
Responsible Role: System Administrator	
Parameter AC-12 (1)(a):	
Implementation Status (check all that apply):	

AC-12 (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	

AC-12 (1) 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: System Administrator	
Parameter AC-14(a):	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

AC-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	

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: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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: System Administrator	

AC-17 (2)	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-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: System Administrator	
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)	

AC-17 (3)	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 (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: System Administrator	
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	

AC-17 (4) What is the solution and how is it implemented?	
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: System Administrator	
Parameter AC-17 (9):	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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: System Administrator	
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	

AC-18 (1)	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	

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

AC-18 (3) CONTROL ENHANCEMENT (H)

The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

AC-18 (3)	Control Summary Information
Responsible Role: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (3) What is the solution and how is it implemented?

AC-18 (4) CONTROL ENHANCEMENT (H)

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

AC-18 (4)	Control Summary Information
Responsible Role: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (4) What is the solution and how is it implemented?

AC-18 (5) CONTROL ENHANCEMENT (H)

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

AC-18 (5)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AC-18 (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	

AC-18 (5) 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 ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:	
Parameter AC-20 (2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AC-20 (2)	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-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 ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

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

13.2. Awareness and Training (AT)

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

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 annually*]; and
(2) Security awareness and training procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AT-1	Control Summary Information
Responsible Role:	

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

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

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:	
Parameter AT-2(c):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

AT-2	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	

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

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

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

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

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

AT-3 (3) CONTROL ENHANCEMENT (H)

The organization includes practical exercises in security training that reinforce training objectives.

AT-3 (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	

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

AT-3 (4) CONTROL ENHANCEMENT (H)

The organization provides training to its personnel on [*FedRAMP Assignment: malicious code indicators as defined by organization incident policy/capability*] to recognize suspicious communications and anomalous behavior in organizational information systems.

AT-3 (4)	Control Summary Information
Responsible Role:	
Parameter AT-3 (4):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

AT-3 (4)	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	

AT-3 (4) What is the solution and how is it implemented?

AT-4 Security Training Records (H)

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 five (5) years or 5 years after completion of a specific training program*].

AT-4	Control Summary Information
Responsible Role:	
Parameter AT-4(b):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

AT-4	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	

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

13.3. Audit and Accountability (AU)

AU-1 Audit and Accountability Policy and Procedures (H)

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 least annually*]; and

(2) Audit and accountability procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AU-1	Control Summary Information
Responsible Role: CISO	
Parameter AU-1(a): System Manager	
Parameter AU-1(b)(1): Annually	
Parameter AU-1(b)(2): Annually and whenever a significant change occurs	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned	

AU-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)	

AU-1 What is the solution and how is it implemented?	
Part a	System manager developed Hope Health Care Information System Audit and Accountability Policy referred to NIST SP 800-53 "Audit and Accountability Control Family guidelines"
Part b	System manager reviews and updates HHCIS audit and accountability policy and procedures annually and whenever significant changes occur.

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*];

(b) Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

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

(d) Determines that the following events are to be audited within the information system: [*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: System Administrator	

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

AU-2 What is the solution and how is it implemented?	
Part a	Information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
Part b	System administrator 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.
Part c	Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
Part d	Organization-defined subset of the auditable events defined in AU-2(a) to be audited continually for each identified event.

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: System Manager	
Parameter AU-2 (3): Annually or whenever significant changes happened in the threat environment.	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-2 (3) What is the solution and how is it implemented?
System managers reviews and updates the list of audited events annually or whenever significant changes happened in the threat environment. The CISO shall communicate changes in the threat environment to the service provider.

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: System Manager	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented	

AU-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	

AU-3 What is the solution and how is it implemented?
System managers configure information systems to generates audit records containing types of events, source and destination network addresses, Source and destination port or protocol identifiers, the outcome of events and identity of the user/subject associated with the event.

AU-3 (1) CONTROL ENHANCEMENT (H)

The information system generates audit records containing the following additional information: [*FedRAMP 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; individual identities of group account users; full-text of privileged commands*]. The audit record types are approved and accepted by the JAB/AO.

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: System Manager	
Parameter AU-3 (1): Additional information: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or	

AU-3 (1)	Control Summary Information
identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
System managers in coordinate with Hope Health Care Information System owners to make more details for information system, include 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; individual identities of group account users; full-text of privileged commands.

AU-3 (2) CONTROL ENHANCEMENT (H)

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*FedRAMP Assignment: all network, data storage, and computing devices*].

AU-3 (2)	Control Summary Information
Responsible Role: System Manager	
Parameter AU-3 (2): All network, data storage, and computing devices.	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AU-3 (2)	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	

AU-3 (2) What is the solution and how is it implemented?
Manage the content of audit records generated by all network, data storage, and computing devices centrally.

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

AU-4 What is the solution and how is it implemented?
Hope Health Care Information System allocates audit record storage capacity and configure auditing to reduce the likelihood of the capacity being exceeded.

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

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

AU-5 (1) CONTROL ENHANCEMENT (H)

The information system provides a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit record storage capacity.

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

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

AU-5 (2) CONTROL ENHANCEMENT (H)

The information system provides an alert in [*FedRAMP Assignment: organization-defined real-time*] to [*FedRAMP Assignment: service provider personnel with authority to address failed audit events*] when the following audit failure events occur: [*FedRAMP Assignment: audit failure events requiring real-time alerts, as defined by organization audit policy*].

AU-5 (2)	Control Summary Information

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

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

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: system administrator	
Parameter AU-6 (a)-1: once a week	
Parameter AU-6 (a)-2: organization-defined inappropriate and unusual activity	
Parameter AU-6 (b): system 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-6 What is the solution and how is it implemented?	
Part a	System administrator reviews and analyzes information audit records weekly for indications of organization-defined inappropriate and unusual activity.
Part b	System administrator reports findings to system manager.

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: system manager	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AU-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	

AU-6 (1) What is the solution and how is it implemented?
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 (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: SO, IO	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
SOs, in coordination with IOs, for HHICS-operated systems, and SMs, in coordination with IOs, for systems operated on behalf of the HHICS, shall ensure that service providers: a) Analyze and correlate audit records across different repositories to gain HHICS-wide situational awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system).

AU-6 (4) CONTROL ENHANCEMENT (H)

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

AU-6 (4)	Control Summary Information
Responsible Role: SO	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (4) What is the solution and how is it implemented?
TSO make sure the information system provides the capability to centrally review and analyze audit records from multiple components within the system.

AU-6 (5) CONTROL ENHANCEMENT (H)

The organization integrates analysis of audit records with analysis of [*FedRAMP Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; penetration test data;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

AU-6 (5)	Control Summary Information
Responsible Role: SO	
Parameter AU-6 (5): organization-defined data and information collected from other sources	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☒ Provided by Customer (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 (5) What is the solution and how is it implemented?
SOs, in coordination with IOs, for HHICS -operated systems, and SMs, in coordination with IOs, for systems operated on behalf of the HHICS, shall ensure that service providers: a) Integrate analysis of audit records with analysis of vulnerability scan information, performance data, information system and insider threats monitoring information, monitoring information from scanning and Intrusion Detection and Prevention System (IDPS) tools, and data/information collected from other sources to enhance the ability to identify inappropriate or unusual activity further.

AU-6 (6) CONTROL ENHANCEMENT (H)

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

AU-6 Additional FedRAMP Requirements and Guidance:

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

AU-6 (6)	Control Summary Information
Responsible Role: system manager	
Implementation Status (check all that apply):	

AU-6 (6)	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	

AU-6 (6) What is the solution and how is it implemented?
SOs, in coordination with IOs, for HHICS -operated systems, and SMs, in coordination with IOs, for systems operated on behalf of the HHICS, shall ensure that service providers: a) Correlate information from audit records with information obtained from monitoring physical access to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity further.

AU-6 (7) CONTROL ENHANCEMENT (H)

The organization specifies the permitted actions for each [*FedRAMP Selection (one or more): information system process; role; user*] associated with the review, analysis, and reporting of audit information.

AU-6 (7)	Control Summary Information
Responsible Role: system manager	
Parameter AU-6 (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	

AU-6 (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	

AU-6 (7) What is the solution and how is it implemented?
After reviewing and analyzing, system manager reports the audit information to SO.

AU-6 (10) CONTROL ENHANCEMENT (H)

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

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

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

AU-6 (10) What is the solution and how is it implemented?
SO adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

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: system 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-7 What is the solution and how is it implemented?	
Part a	SOs, in coordination with IOs, for HHICS -operated systems, and SMs, in coordination with IOs, for systems operated on behalf of the HHICS, shall ensure that service providers: a) Configure the information system to provide an audit reduction5 and report generation capability that: i) Supports near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents; and ii) Does not alter the original content or time recording of audit records.
Part b	System manager and system administrator configure the information system to make sure the original content or time ordering of audit records.

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: system manager	
Parameter AU-7 (1): audit log by username, location, application name, date, and time, or other applicable parameters;	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
System manager make sure that: a) Employ automated tools to review audit records. The following audit analysis tools may be used: i) Audit analysis tools based on attack signature, variance techniques, and audit reduction methodologies to detect intrusion ii) Data reduction audit tools to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data iii) Query applications that have the ability to query an audit log by username, location, application name, date, and time, or other applicable parameters; and have the ability to execute reports with the results of the query b) Ensure information systems provide the capability to process audit records for events of interest based on selectable event criteria including event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.

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: System Administrator	
Parameter AU-8(b): 20 seconds granularity of time measurement.	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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	System administrator configure HHCIS to use internal system clocks to generate time stamps which include date and time for audit records.
Part b	Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets 20 seconds granularity of time measurement.

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: System Administrator	
Parameter AU-8(1)(a)-1: primary authoritative time source: time-ag.nist.gov, secondary authoritative time source: time.-ab.nist.gov	
Parameter AU-8(1)(a)-2: Daily	
Parameter AU-8(1)(b): 20 seconds	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☒ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-8 (1) What is the solution and how is it implemented?	
Part a	Compares the internal information system clocks with primary and secondary timeservers.
Part b	Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than 20 seconds.

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: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?
The system administrator protects audit information and audit tools from unauthorized access, modification, and deletion.

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

AU-9 (2) What is the solution and how is it implemented?
Configure information systems to back up audit records nightly onto a physically different system or system component than the system or component being audited.

AU-9 (3) CONTROL ENHANCEMENT (H)

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

AU-9 (3)	Control Summary Information
Responsible Role: System Administrator	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

AU-9 (3)	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-9 (3) What is the solution and how is it implemented?
Implement cryptographic mechanisms on information systems to protect the integrity of audit information and audit tools.

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: System Administrator	
Parameter AU-9(4): system administrators, security officials	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-9 (4) What is the solution and how is it implemented?
Authorize access to management of audit functionality to authorized system administrators, and the designated security

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

AU-10 Non-repudiation (H)

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*FedRAMP Assignment: minimum actions including the addition, modification, deletion, approval, sending, or receiving of data*].

AU-10	Control Summary Information
Responsible Role: system administrator	
Parameter AU-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	

AU-10 What is the solution and how is it implemented?
System administrator configures information systems to protect against an individual (or a process acting on behalf of an individual) falsely denying having performed a particular action. Actions covered by non-repudiation includes, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract)

AU-11 Audit Record Retention (H)

The organization retains audit records for [*FedRAMP Assignment: at least one (1) year*] 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: system manager	
Parameter AU-11: one 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	

AU-11 What is the solution and how is it implemented?
System manager archives audit records for a period of no less than one year with 90 days online and the remaining time stored offline. Besides, Transfer audit records for remote access devices from the devices to a central log server where they are retained for up to three years.

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: system manager	
Parameter AU-12(a): Desktop and laptop computers (end-user environment) ii) Servers (e.g., file and print, web, firewalls, terminal) iii) Network components (e.g., switches, routers wireless)	
Parameter AU-12(b): ISSO, ISO, SO and system administrator	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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	System manager and ayatem administrator configure information systems to provide audit record generation capability for the list of auditable events defined in AU-2 with content prescribed in AU-3 on, at a minimum, the following information system components: i) Desktop and laptop computers (end-user environment) ii) Servers (e.g., file and print, web, firewalls, terminal) iii) Network components (e.g., switches, routers wireless)
Part b	System manager allows ISSO, ISO, SO and system administrators to select which auditable events are to be audited by specific components of the information system
Part c	HCCIS Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

AU-12 (1) CONTROL ENHANCEMENT (H)

The information system compiles audit records from [*FedRAMP Assignment: all network, data storage, and computing devices*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

AU-12 (1)	Control Summary Information
Responsible Role: system administrator	
Parameter AU-12 (1)-1: all network, data storage, and computing devices	
Parameter AU-12 (1)-2: physical	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (1) What is the solution and how is it implemented?
System administrator configure information systems to compile audit records into a system-wide (physical) audit trail that is time-correlated to within acceptable levels of tolerance for relationship between time stamps of individual records in the audit trail.

AU-12 (3) CONTROL ENHANCEMENT (H)

The information system provides the capability for [*FedRAMP Assignment*: *service provider-defined individuals or roles with audit configuration responsibilities*] to change the auditing to be performed on [*FedRAMP Assignment*: *all network, data storage, and computing devices*] based on [*Assignment*: *organization-defined threat situations*] within [*Assignment*: *organization-defined time thresholds*].

AU-12 (3)	Control Summary Information
Responsible Role: system manager	
Parameter AU-12 (3)-1: system administrators	
Parameter AU-12 (3)-2: all network, data storage, and computing devices	
Parameter AU-12 (3)-3: failure of audit, unauthorized login and so on	
Parameter AU-12 (3)-4: ten minutes	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☒ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AU-12 (3) What is the solution and how is it implemented?
System manager configures information systems to provide the capability for system administrators to change the auditing to be performed on all applicable system components based on policy, procedures and standards in coordination with the applicable ISSO, ISO and SO.

13.4. Security Assessment and Authorization (CA)

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

The organization:

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

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

(2) Procedures to facilitate the implementation of the security assessment and

authorization policy and associated security assessment and authorization controls; and

(b) Reviews and updates the current:

(1) Security assessment and authorization policy [*FedRAMP Assignment: at least annually*]; and
(2) Security assessment and authorization procedures [*FedRAMP Assignment: at least at least annually or whenever a significant change occurs*].

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

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

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) ☐ Provided by Customer (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:	

CA-2 (3)	Control Summary Information
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;

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

(c) 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 Table 11- 1 System Interconnections 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 (H)

The organization employs [*FedRAMP Selection: deny-all, permit by exception*] policy for allowing [*FedRAMP Assignment: any 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

(b) 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;

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

(c) 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;

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

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

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

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

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

(g) Reporting the security status of organization and the information system to [*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):	

CA-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	

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)	

CA-7 Req.	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-7 What is the solution and how is it implemented?	
Req. 1	
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-7 (3) CONTROL ENHANCEMENT (H)

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

CA-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	

CA-7 (3) 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:	

CA-8	Control Summary Information
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	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific	

CA-8 (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	

CA-8 (1) 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

(b) 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 (H)

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 annually*]; and
(2) Configuration management procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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 (H)

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

(a) [*FedRAMP Assignment: at least annually or when a significant change occurs*];

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

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

CM-2 (1) (a) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, Page F-7.

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:	

CM-2 (2)	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	

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

CM-2 (3) CONTROL ENHANCEMENT (H)

The organization retains [*FedRAMP Assignment: the previously approved baseline configuration of IS components*] 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)	

CM-2 (3)	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-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

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

CM2 (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;

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

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

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

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

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

Guidance: In accordance with record retention policies and procedures.

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

(g) Coordinates and provides oversight for configuration change control activities through [*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:	

CM-3	Control Summary Information
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) ☐ 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-3 (1) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [*Assignment: organization-defined configuration management approval authorities*] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [*FedRAMP Assignment: organization agreed upon time period*];

(d) Prohibit changes to the information system until designated approvals are received;

(e) Document all changes to the information system; and

(f) Notify [*FedRAMP Assignment: organization-defined configuration management approval authorities*] when approved changes to the information system are completed.

CM-3 (1)	Control Summary Information
Responsible Role:	
Parameter CM-3 (1)(b):	
Parameter CM-3 (1)(c):	
Parameter CM-3 (1)(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	

CM-3 (1) What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

CM-3 (2) CONTROL ENHANCEMENT (M)(H)

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

CM-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	

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

CM-3 (4) ENHANCEMENT (H)

The organization requires an information security representative to be a member of the [*FedRAMP Assignment: configuration control board (CCB) or similar (as defined in CM-3)*].

CM-3 (4)	Control Summary Information
Responsible Role:	
Parameter CM-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	

CM-3 (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	

CM-3 (4) What is the solution and how is it implemented?

CM-3 (6) ENHANCEMENT (H)

The organization ensures that cryptographic mechanisms used to provide [*FedRAMP Assignment: all security safeguards that rely on cryptography*] are under configuration management.

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

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

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-4 (1) CONTROL ENHANCEMENT (H)

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

CM-4 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

CM-4 (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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (1) 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	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (2) CONTROL ENHANCEMENT (H)

The organization reviews information system changes [*FedRAMP Assignment: at least every thirty (30) days*] and [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.

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

CM-5 (2)	Control Summary Information
Parameter CM-5 (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	

CM-5 (2) 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	

CM-5 (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	

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)	

CM-5 (5)	Control Summary Information
☐ 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.

(b) Implements the configuration settings;

(c) Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

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

CM-6	Control Summary Information
Responsible Role:	
Parameter CM-6 (a)-1:	
Parameter CM-6 (a)-2:	

CM-6	Control Summary Information
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	

CM-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	

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

CM-6 (2) CONTROL ENHANCEMENT (H)

The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

CM-6 (2)	Control Summary Information
Responsible Role:	
Parameter CM-6 (2)-1:	
Parameter CM-6 (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	

CM-6 (2) 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)	

CM-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	

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?

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 (H)

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 quarterly 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 ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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) ☐ Provided by Customer (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 (2) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

CM-8 (2)	Control Summary Information

CM-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	

CM-8 (2) 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	

CM-8 (3)	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	

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

CM-8 (4) CONTROL ENHANCEMENT (H)

The organization includes in the information system component inventory information, a means for identifying by [*Selection (one or more): name;* [*FedRAMP Assignment: position and role*]], individuals responsible/accountable for administering those components.

CM-8 (4)	Control Summary Information
Responsible Role:	
Parameter CM-8 (4):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)	

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

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

CM-11	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	

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

CM-11 (1) CONTROL ENHANCEMENT (H)

The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.

CM-11 (1)	Control Summary Information
Responsible Role:	
Parameter CM-11 (1):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

CM-11 (1)	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	

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

13.6. Contingency Planning (CP)

CP-1 Contingency Planning Policy and Procedures (H)

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 annually*]; and
2. Contingency planning procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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

CP-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)	

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

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*];

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

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

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

(e) 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;

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

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

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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

CP-2 (2)	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	

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

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

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

CP-2 (4) CONTROL ENHANCEMENT (H)

The organization plans for the resumption of all missions and business functions within [*FedRAMP Assignment: time period defined in service provider and organization Service Level Agreement (SLA)*] of contingency plan activation.

CP-2 (4)	Control Summary Information
Responsible Role:	
Parameter CP-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	

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

CP-2 (5) CONTROL ENHANCEMENT (H)

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

CP-2 (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	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ 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-2 (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	

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

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;

(b) When required by information system changes; and

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

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

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

CP-3 (1) CONTROL ENHANCEMENT (H)

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

CP-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	

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

CP-4 Contingency Plan Testing (H)

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.

(b) Reviews the contingency plan test results; and

(c) Initiates corrective actions, if needed.

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

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

CP-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:	

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

CP-4 (2) CONTROL ENHANCEMENT (H)

The organization tests the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

CP-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	

CP-4 (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-4 (2) What is the solution and how is it implemented?	
Part a	
Part b	

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

(b) Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

CP-6	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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 (2) CONTROL ENHANCEMENT (H)

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

CP-6 (2)	Control Summary Information
Responsible Role:	

CP-6 (2)	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-6 (2) 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)	

CP-6 (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	

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.

(b) Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

(c) Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

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	

CP-7	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	

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)	

CP-7 (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	

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-7 (4) CONTROL ENHANCEMENT (H)

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

CP-7 (4)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

CP-7 (4)	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	

CP-7 (4) 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	

CP-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	

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

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

CP-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	

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-8 (3) CONTROL ENHANCEMENT (H)

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

CP-8 (3)	Control Summary Information

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

CP-8 (4) CONTROL ENHANCEMENT (H)

The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtains evidence of contingency testing/training by providers [*FedRAMP Assignment: annually*].

CP-8 (4)	Control Summary Information
Responsible Role:	
Parameter CP-8 (4)(c):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

CP-8 (4)	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-8 (4) What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

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).

(b) 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).

(c) 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).

(d) 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):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (H)

The organization tests backup information [*FedRAMP Assignment: at least monthly*] 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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (2) CONTROL ENHANCEMENT (H)

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

CP-9 (2)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

CP-9 (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	

CP-9 (2) 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-9 (5) CONTROL ENHANCEMENT (H)

The organization transfers information system backup information to the alternate storage site [*FedRAMP Assignment: time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA*].

CP-9 (5)	Control Summary Information
Responsible Role:	
Parameter CP-9 (5):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

CP-9 (5) 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 ☐ Service Provider Hybrid (Corporate and System Specific)	

CP-10 (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	

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

CP-10 (4) CONTROL ENHANCEMENT (H)

The organization provides the capability to restore information system components within [*FedRAMP Assignment: time period consistent with the restoration time-periods defined in the service provider and organization SLA*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

CP-10 (4)	Control Summary Information
Responsible Role:	
Parameter CP-10 (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	

CP-10 (4) What is the solution and how is it implemented?

13.7. Identification and Authentication (IA)

IA-1 Identification and Authentication Policy and Procedures (H)

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 annually*]; and
(2) Identification and authentication procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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

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

IA-2 (1) 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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

IA-2 (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	

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

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

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

IA-2 (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 ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

IA-2 (4) CONTROL ENHANCEMENT (H)

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

IA-2 (4)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

IA-2 (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	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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

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

IA-2 (9) CONTROL ENHANCEMENT (H)

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

IA-2 (9)	Control Summary Information
Responsible Role:	

IA-2 (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	

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

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:	
Parameter IA-2 (11):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)	

IA-2 (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	

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

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:	
Parameter IA-3-1:	
Parameter IA-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	

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

IA-4 Identifier Management (H)

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

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

(b) Selecting an identifier that identifies an individual, group, role, or device;

(c) Assigning the identifier to the intended individual, group, role, or device;

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

(e) Disabling the identifier after [*FedRAMP Assignment: thirty-five (35) days (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:	
Parameter IA-4(a):	
Parameter IA-4(d):	
Parameter IA-4(e):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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

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

IA-5 Authenticator Management (H)

The organization manages information system authenticators by:

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

(b) Establishing initial authenticator content for authenticators defined by the organization;

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

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

(e) Changing default content of authenticators prior to information system installation;

(f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

(g) Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*].

(h) Protecting authenticator content from unauthorized disclosure and modification;

(i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

(j) 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 3. 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 ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

IA-5	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	

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 (H)

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(b) Enforces at least the following number of changed characters when new passwords are created: [*FedRAMP Assignment: at least fifty percent (50%)*];

(c) Stores and transmits only cryptographically-protected passwords;

(d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization- defined numbers for lifetime minimum, lifetime maximum*];

(e) Prohibits password reuse for [*FedRAMP Assignment: twenty-four (24)*] generations; and

(f) 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

IA-5 (3)	Control Summary Information
Responsible Role:	
Parameter IA-5 (3)-1:	
Parameter IA-5 (3)-2:	
Parameter IA-5 (3)-3:	
Parameter IA-5 (3)-4:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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 (H)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*FedRAMP Assignment: complexity as identified in IA-5 (1) Control Enhancement (H) Part A*].

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)	

IA-5 (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	

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)	

IA-5 (6)	Control Summary Information
☐ 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 (8) CONTROL ENHANCEMENT (H)

The organization implements [*FedRAMP Assignment: different authenticators on different systems*] to manage the risk of compromise due to individuals having accounts on multiple information systems.

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

IA-5 (8) 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-5 (13) CONTROL ENHANCEMENT (H)

The information system prohibits the use of cached authenticators after [*Assignment: organization-defined time period*].

IA-5 (13)	Control Summary Information
Responsible Role:	
Parameter IA-5 (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	

IA-5 (13) 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	

IA-7	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	

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

IA-8	Control Summary Information
☐ 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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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

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

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

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 ☐ Service Provider Hybrid (Corporate and System Specific)	

IA-8 (3)	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	

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

The organization:

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

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

(b) Reviews and updates the current:

(1) Incident response policy [*FedRAMP Assignment: at least annually*]; and
(2) Incident response procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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 (H)

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 [*FedRAMP Assignment: ten (10) days*] of assuming an incident response role or responsibility;

(b) When required by information system changes; and

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

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

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

IR-2 (1) CONTROL ENHANCEMENT (H)

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

IR-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	

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

IR-2 (2) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

IR-2 (2)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

IR-2 (2)	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	

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

IR-3 Incident Response Testing (H)

The organization tests the incident response capability for the information system [*FedRAMP Assignment: at least every six (6) months*] 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:	
Parameter IR-3-1:	
Parameter IR-3-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

IR-3	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	

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

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

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

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

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

IR-4 (2) CONTROL ENHANCEMENT (H)

The organization includes dynamic reconfiguration of [*FedRAMP Assignment: all network, data storage, and computing devices*] as part of the incident response capability.

IR-4 (2)	Control Summary Information
Responsible Role:	
Parameter IR-4 (2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

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

IR-4 (3) CONTROL ENHANCEMENT (H)

The organization identifies [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incident*] to ensure continuation of organizational missions and business functions.

IR-4 (3)	Control Summary Information
Responsible Role:	
Parameter IR-4 (3)-1	
Parameter IR-4 (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	

IR-4 (3) What is the solution and how is it implemented?

IR-4 (4) CONTROL ENHANCEMENT (H)

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

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

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

IR-4 (6) CONTROL ENHANCEMENT (H)

The organization implements incident handling capability for insider threats.

IR-4 (6)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply):	

IR-4 (6)	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	

IR-4 (6) What is the solution and how is it implemented?

IR-4 (8) CONTROL ENHANCEMENT (H)

The organization implements incident handling capability for insider threats.

The organization coordinates with [*FedRAMP Assignment: external organizations including consumer incident responders and network defenders and the appropriate consumer incident response team (CIRT)/ Computer Emergency Response Team (CERT) (such as US-CERT, DoD CERT, IC CERT)*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross- organization perspective on incident awareness and more effective incident responses.

IR-4 (8)	Control Summary Information
Responsible Role:	
Parameter IR-4 (8)-1:	
Parameter IR-4 (8)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

IR-4 (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	

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

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

The organization tracks and documents information system security incidents.

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

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

IR-5 (1) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

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

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

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

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

IR-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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

IR-6 (1)	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	

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

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

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

IR-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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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

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

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*].

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):	
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	

IR-8 What is the solution and how is it implemented?	
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)	

IR-9	Control Summary Information
☐ 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 ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (H)

The organization provides information spillage response training [*FedRAMP Assignment: at least annually*].

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:	

IR-9 (3)	Control Summary Information
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):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ 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-9 (4)	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	

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

13.9. Maintenance (MA)

MA-1 System Maintenance Policy and Procedures (H)

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 annually*]; and
(2) System maintenance procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

MA-1	Control Summary Information
Responsible Role:	
Parameter MA-1(a):	
Parameter MA-1(b)(1):	
Parameter MA-1(b)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

MA-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)	

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):	

MA-2	Control Summary Information
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-2 (2) CONTROL ENHANCEMENT (H)

The organization:

(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

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

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

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 ☐ Not applicable	
Control Origination (check all that apply):	

MA-3	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	

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):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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	

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

MA-4 (3) CONTROL ENHANCEMENT (H)

The organization:

(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

MA-4 (3)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

MA-4 (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-4 (3) What is the solution and how is it implemented?	
Part a	
Part b	

MA-4 (6) ENHANCEMENT (H)

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

MA-4 (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)	

MA-4 (6)	Control Summary Information
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

MA-4 (6) 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	
Part b	
Part c	

MA-5 (1) CONTROL ENHANCEMENT (H)

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

(a) 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)	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 (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) Media protection policy [*FedRAMP Assignment: at least annually*]; and
(2) Media protection procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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 (H)

The organization restricts access to [*FedRAMP Assignment: any digital and non-digital media deemed sensitive*] to [*Assignment: organization-defined personnel or roles*].

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

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

MP-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:	
Parameter MP-3(b)-1:	
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	
Part b	

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.

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

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

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

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.

(b) Maintains accountability for information system media during transport outside of controlled areas;

(c) Documents activities associated with the transport of information system media; and

(d) Restricts the activities associated with transport of information system media to authorized personnel.

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

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

MP-6 Media Sanitization and Disposal (H)

The organization:

(a) Sanitizes [*Assignment: organization-defined information system media]* prior to disposal, release out of organizational control, or release for reuse using *[FedRAMP Assignment: techniques and procedures IAW NIST SP 800-88 R1, Appendix A - Minimum Sanitization Recommendations*] in accordance with applicable federal and organizational standards and policies; and

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

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

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

MP-6 (1) CONTROL ENHANCEMENT (H)

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

MP-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	

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

MP-6 (2) CONTROL ENHANCEMENT (H)

The organization tests sanitization equipment and procedures [*FedRAMP Assignment: at least every six (6) months*] 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:	
Parameter MP-6(2):	
Implementation Status (check all that apply):	

MP-6 (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	

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

MP-6 (3) CONTROL ENHANCEMENT (H)

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

MP-6 (3)	Control Summary Information
Responsible Role:	
Parameter MP-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	

MP-6 (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	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific)	

MP-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	

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 (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	

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 (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) Physical and environmental protection policy [*FedRAMP Assignment: at least annually*]; and
(2) Physical and environmental protection procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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	

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

PE-2 Physical Access Authorizations (H)

The organization:

(a) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

(b) Issues authorization credentials for facility access;

(c) Reviews the access list detailing authorized facility access by individuals [*FedRAMP Assignment: at least every ninety (90) days*]; and

(d) 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	

PE-2 What is the solution and how is it implemented?	
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*];

(a) Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

(b) Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

(c) Escorts visitors and monitors visitor activity [*FedRAMP Assignment: in all circumstances within restricted access area where the information system resides*];

(d) Secures keys, combinations, and other physical access devices;

(e) Inventories [*Assignment: organization-defined physical access devices*] every [*FedRAMP Assignment: at least annually*]; and

(f) 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:	

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

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

PE-3 (1) CONTROL ENHANCEMENT (H)

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing components of the information system*].

PE-3 (1)	Control Summary Information
Responsible Role:	

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

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

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	

PE-4	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	

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)	

PE-5	Control Summary Information
☐ 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)	

PE-6	Control Summary Information
☐ 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-6 (4) CONTROL ENHANCEMENT (H)

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

PE-6 (4)	Control Summary Information
Responsible Role:	
Parameter PE-6 (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	

PE-6 (4) 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 ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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-8 (1) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

PE-8 (1)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

PE-8 (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) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (1) What is the solution and how is it implemented?

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)	

PE-9	Control Summary Information
☐ 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-11 (1) CONTROL ENHANCEMENT (H)

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

PE-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	

PE-11 (1) 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):	

PE-12	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	

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)	

PE-13	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	

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

PE-13 (1) CONTROL ENHANCEMENT (H)

The organization employs fire detection devices/systems for the information system that activate automatically and notify [*FedRAMP Assignment: service provider building maintenance/physical security personnel*] and [*FedRAMP Assignment: service provider emergency responders with incident response responsibilities*] in the event of a fire.

PE-13 (1)	Control Summary Information
Responsible Role:	
Parameter PE-13 (1)-1:	
Parameter PE-13 (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	

PE-13 (1) 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 ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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:	

PE-14	Control Summary Information
Parameter PE-14(a):	
Parameter PE-14(b):	
Parameter PE-14(b) Additional:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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	

PE-14 (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	

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)	

PE-15	Control Summary Information
☐ 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-15 (1) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*FedRAMP Assignment: service provider building maintenance /physical security personnel*].

PE-15 (1)	Control Summary Information
Responsible Role:	
Parameter PE-15 (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	

PE-15 (1) 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 ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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;

(b) Assesses as feasible, the effectiveness of security controls at alternate work sites; and

(c) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

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	

PE-18 Location of Information System Components (H)

The organization positions information system components within the facility to minimize potential damage from [*FedRAMP Assignment: physical and environmental hazards identified during threat assessment*] and to minimize the opportunity for unauthorized access.

PE-18	Control Summary Information
Responsible Role:	
Parameter PE-18:	
Implementation Status (check all that apply): ☐ Implemented	

PE-18	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	

PE-18 What is the solution and how is it implemented?

13.12. Planning (PL)

PL-1 Security Planning Policy and Procedures (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) Security planning policy [*FedRAMP Assignment: at least annually*]; and
(2) Security planning procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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

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

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

The organization:

(a) Develops a security plan for the information system that:

(1) Is consistent with the organization's enterprise architecture;
(2) Explicitly defines the authorization boundary for the system;
(3) Describes the operational context of the information system in terms of missions and business processes;
(4) Provides the security categorization of the information system including supporting rationale;
(5) Describes the operational environment for the information system and relationships with or connections to other information;
(6) Provides an overview of the security requirements for the system;
(7) Identifies any relevant overlays, if applicable;
(8) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

(9) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

(b) Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

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

(d) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

(e) Protects the security plan from unauthorized disclosure and modification.

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

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

PL-2 What is the solution and how is it implemented?	
Part e	

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

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

PL-4 Rules of Behavior (H)

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;

(b) 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;

(c) Reviews and updates the rules of behavior [*FedRAMP Assignment: annually*]; and

(d) Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

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

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

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

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

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;

(b) 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.

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

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

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

13.13. Personnel Security (PS)

PS-1 Personnel Security Policy and Procedures (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) Personnel security policy [*FedRAMP Assignment: at least annually*]; and
(2) Personnel security procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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	

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

PS-2 Position Categorization (H)

The organization:

(a) Assigns a risk designation to all positions;

(b) Establishes screening criteria for individuals filling those positions; and

(c) Reviews and revises position risk designations [*FedRAMP Assignment: at least annually*].

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

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

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

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

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

PS-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

(b) Satisfy [*FedRAMP Assignment: personnel screening criteria – as required by specific information*].

PS-3 (3)	Control Summary Information
Responsible Role:	
Parameter PS-3 (3)(b):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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	
Part b	

PS-4 Personnel Termination (H)

The organization, upon termination of individual employment:

(a) Disables information system access within [*FedRAMP Assignment: eight (8) hours*];

(b) Terminates/revokes any authenticators/credentials associated with the individual;

(c) Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

(d) Retrieves all security-related organizational information system-related property;

(e) Retains access to organizational information and information systems formerly controlled by terminated individual; and

(f) Notifies [*Assignment: organization-defined personnel or roles]* within [*Assignment: organization-defined time period*].

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

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

PS-4 What is the solution and how is it implemented?	
Part d	
Part e	
Part f	

PS-4 (2) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to notify [*FedRAMP Assignment: access control personnel responsible for disabling access to the system*] upon termination of an individual.

PS-4 (2)	Control Summary Information
Responsible Role:	
Parameter PS-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	

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

PS-5 Personnel Transfer (H)

The organization:

(a) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

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

(c) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

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

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

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

PS-6 Access Agreements (H)

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

(c) Ensures that individuals requiring access to organizational information and information systems:

(1) Sign appropriate access agreements prior to being granted access; and
(2) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*FedRAMP Assignment: at least annually and any time there is a change to the user's level of access*].

PS-6	Control Summary Information
Responsible Role:	
Parameter PS-6(b):	
Parameter PS-6(c)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)	

PS-6	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	

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

PS-7 Third-Party Personnel Security (H)

The organization:

(a) Establishes personnel security requirements including security roles and responsibilities for third-party providers;

(b) Requires third-party providers to comply with personnel security policies and procedures established by the organization;

(c) Documents personnel security requirements;

(d) Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*FedRAMP Assignment: terminations: immediately; transfers: within twenty-four (24) hours*]; and

(e) Monitors provider compliance.

PS-7	Control Summary Information
Responsible Role:	
Parameter PS-7(d)-1:	
Parameter PS-7(d)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

PS-7	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	

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

PS-8 Personnel Sanctions (H)

The organization:

(a) Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and

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

PS-8	Control Summary Information
Responsible Role:	
Parameter PS-8(b)-1:	
Parameter PS-8(b)-2:	

PS-8	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	

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

13.14. Risk Assessment (RA)

RA-1 Risk Assessment Policy and Procedures (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) Risk assessment policy [*FedRAMP Assignment: at least annually*]; and
(2) Risk assessment procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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:	

RA-2	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	

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

RA-3 Risk Assessment (H)

The organization:

(a) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

(b) Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*FedRAMP Assignment: security assessment report*]];

(c) Reviews risk assessment results [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*];

(d) Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

(e) 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	

RA-3 What is the solution and how is it implemented?	
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.

(b) 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;

(c) Analyzes vulnerability scan reports and results from security control assessments

(d) 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

(e) Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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

RA-5 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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:	
Parameter RA-5(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

RA-5 (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	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

RA-5 (4) CONTROL ENHANCEMENT (H)

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*FedRAMP Assignment: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions*].

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

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

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:	
Parameter RA-5(5)-1:	

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

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

RA-5 (6)	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	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility)	

RA-5 (8)	Control Summary Information
☐ 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?

RA-5 (10) CONTROL ENHANCEMENT (H)

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

RA-5 (10) Additional FedRAMP Requirements and Guidance:

Guidance: If multiple tools are not used, this control is not applicable.

RA-5 (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	

RA-5 (10) What is the solution and how is it implemented?

13.15. System and Services Acquisition (SA)

SA-1 System and Services Acquisition Policy and Procedures (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) System and services acquisition policy [*FedRAMP Assignment: at least annually*]; and
(2) System and services acquisition procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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	

SA-1 What is the solution and how is it implemented?	
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): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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.

Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.
See http://www.niap-ccevs.org/vpl or
http://www.commoncriteriaportal.org/products.html.

SA-4	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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 (H)

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): at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram; [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): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

SA-4 (10)	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	

SA-4 (10) What is the solution and how is it implemented?

SA-5 Information System Documentation (H)

The organization:

(a) Obtains administrator documentation for the information system, system component, or information system service that describes:

(1) Secure configuration, installation, and operation of the system, component, or service;
(2) Effective use and maintenance of security functions/mechanisms; and
(3) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

(b) Obtains user documentation for the information system, system component, or information system service that describes:

(1) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
(2) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
(3) User responsibilities in maintaining the security of the system, component, or service;

(c) Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;

(d) Protects documentation as required, in accordance with the risk management strategy; and

(e) Distributes documentation to [*FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)*].

SA-5	Control Summary Information
Responsible Role:	

SA-5	Control Summary Information
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):	

SA-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	

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

SA-9 (2)	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 (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)	

SA-9 (4)	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	

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):	

SA-10	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-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)	

SA-10 (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	

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): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)	

SA-11	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	

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

SA-11 (1)	Control Summary Information
☐ 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?

SA-12 Supply Chain Protection (H)

The organization protects against supply chain threats to the information system, system component, or information system service by employing [*FedRAMP Assignment: organization and service provider-defined personnel security requirements, approved HW/SW vendor list/ process, and secure SDLC procedures*] as part of a comprehensive, defense-in-breadth information security strategy.

SA-12	Control Summary Information
Responsible Role:	

SA-12	Control Summary Information
Parameter SA-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	

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

SA-15 Development Process, Standards, and Tools (H)

The organization:

(a) Requires the developer of the information system, system component, or information system service to follow a documented development process that:

(1) Explicitly addresses security requirements;
(2) Identifies the standards and tools used in the development process;
(3) Documents the specific tool options and tool configurations used in the development process; and
(4) Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

(b) Reviews the development process, standards, tools, and tool options/configurations [*FedRAMP Assignment: as needed and as dictated by the current threat posture*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*FedRAMP Assignment: organization and service provider- defined security requirements*].

SA-15	Control Summary Information
Responsible Role:	
Parameter SA-15 (b)-1:	
Parameter SA-15 (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	

SA-15 What is the solution and how is it implemented?	
Part a	
Part b	

SA-16 Developer-Provided Training (H)

The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

SA-16	Control Summary Information
Responsible Role:	
Parameter SA-16:	
Implementation Status (check all that apply): ☐ Implemented	

SA-16	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-16 What is the solution and how is it implemented?

SA-17 Developer Security Architecture and Design (H)

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

(a) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

(b) Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

(c) Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

SA-17	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

SA-17	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	

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

13.16. System and Communications Protection (SC)

SC-1 System and Communications Protection Policy and Procedures (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) System and communications protection policy [*FedRAMP Assignment: at least annually*]; and
(2) System and communications protection procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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 ☐ Alternative implementation ☐ Not applicable	

SC-2	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	

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

SC-3 Security Function Isolation (H)

The information system isolates security functions from non-security functions.

SC-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	

SC-3 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:	
Parameter SC-5-1:	
Parameter SC-5-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

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

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:	

SC-6	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-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:	
Parameter SC-7(b):	
Implementation Status (check all that apply): ☐ Implemented	

SC-7	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	

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

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider 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-7 (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	

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

SC-7 (4) CONTROL ENHANCEMENT (H)

The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy [*FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions*] and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7 (4)	Control Summary Information
Responsible Role:	
Parameter SC-7(4)(e):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific)	

SC-7 (4)	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	

SC-7 (4) What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

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:	
Parameter SC-7(8)-1:	
Parameter SC-7(8)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (8) What is the solution and how is it implemented?

SC-7 (10) CONTROL ENHANCEMENT (H)

The organization prevents the unauthorized exfiltration of information across managed interfaces.

SC-7 (10)	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

SC-7 (10)	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	

SC-7 (10) What is the solution and how is it implemented?

SC-7 (12) CONTROL ENHANCEMENT (H)

The organization implements [*FedRAMP Assignment: Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall*] at [*Assignment: organization-defined information system components*].

SC-7 (12)	Control Summary Information
Responsible Role:	
Parameter SC-7(12)-1:	
Parameter SC-7(12)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility)	

SC-7 (12)	Control Summary Information
☐ 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?

SC-7 (13) CONTROL ENHANCEMENT (H)

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 security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

Guidance: Examples include: information security tools, mechanisms, and support components such as, but not limited to public key infrastructure (PKI), patching infrastructure, cyber defense tools, special purpose gateway, vulnerability tracking systems, internet access points (IAPs); network element and data center administrative/management traffic; demilitarized zones (DMZs), Server farms/computing centers, centralized audit log servers, etc.

SC-7 (13)	Control Summary Information
Responsible Role:	
Parameter SC-7(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	

SC-7 (13)	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	

SC-7 (13) What is the solution and how is it implemented?

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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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?

SC-7 (20) CONTROL ENHANCEMENT (H)

The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.

SC-7 (20)	Control Summary Information
Responsible Role:	
Parameter SC-7 (20):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (20) What is the solution and how is it implemented?

SC-7 (21) CONTROL ENHANCEMENT (H)

The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined mission and/or business functions*].

SC-7 (21)	Control Summary Information
Responsible Role:	
Parameter SC-7 (21)-1:	

SC-7 (21)	Control Summary Information
Parameter SC-7 (21)-2:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-7 (21) What is the solution and how is it implemented?

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	

SC-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	

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)	

SC-8 (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	

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

SC-10 Network Disconnect (H)

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 ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for 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:	
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 (1) CONTROL ENHANCEMENT (H)

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

SC-12 (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	

SC-12 (1) 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):	

SC-12 (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	

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) ☐ 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	

SC-17	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	

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)	

SC-18	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-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

(b) Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

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

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

SC-20 What is the solution and how is it implemented?	
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:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	

SC-23	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	

SC-23 What is the solution and how is it implemented?

SC-23 (1) ENHANCEMENT (H)

The information system invalidates session identifiers upon user logout or other session termination.

SC-23 (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	

SC-23 (1) What is the solution and how is it implemented?

SC-24 Fail in Known State (H)

The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

SC-24	Control Summary Information
Responsible Role:	
Parameter SC-24-1:	
Parameter SC-24-2:	
Parameter SC-24-3:	
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-24 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 ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (H)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*FedRAMP Assignment: all information system components storing customer data deemed sensitive*]

SC-28 (1)	Control Summary Information
Responsible Role:	

SC-28 (1)	Control Summary Information
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):	

SC-39	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	

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 (H)

The organization:

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

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

(b) Reviews and updates the current:

(1) System and information integrity policy [*FedRAMP Assignment: at least annually*]; and
(2) System and information integrity procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

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

SI-1	Control Summary Information
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;

(b) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

(c) Installs security-relevant software and firmware updates within [*FedRAMP Assignment: thirty 30 days of release of updates*] of the release of the updates; and

(d) 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	

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

SI-2 (1) CONTROL ENHANCEMENT (H)

The organization centrally manages the flaw remediation process.

SI-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	

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

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

(b) 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 (H)

The organization:

(a) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

(b) Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

(c) Configures malicious code protection mechanisms to:

(1) Perform periodic scans of the information system [*FedRAMP Assignment: at least weekly*] and real-time scans of files from external sources at [*FedRAMP Assignment: to include endpoints*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

(2) [*FedRAMP Assignment: to include blocking and quarantining malicious code and alerting administrator or defined security personnel near-real-time*] in response to malicious code detection; and

(d) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

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	

SI-3 What is the solution and how is it implemented?	
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): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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	

SI-3 (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	

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:

(1) Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
(2) Unauthorized local, network, and remote connections;

(b) Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

(c) Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

(d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

(e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

(f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

(d) 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 ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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	

SI-4 (2)	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-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)	

SI-4 (4)	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	

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 ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (11) CONTROL ENHANCEMENT (H)

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.

SI-4 (11)	Control Summary Information
Responsible Role:	
Parameter SI-4 (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	

SI-4 (11) 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	

SI-4 (16)	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	

SI-4 (16) What is the solution and how is it implemented?

SI-4 (18) CONTROL ENHANCEMENT (H)

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system* (*e.g., subnetworks, subsystems*)] to detect covert exfiltration of information.

SI-4 (18)	Control Summary Information
Responsible Role:	
Parameter SI-4 (18):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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 (18) What is the solution and how is it implemented?

SI-4 (19) CONTROL ENHANCEMENT (H)

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

SI-4 (19)	Control Summary Information
Responsible Role:	
Parameter SI-4 (19)-1:	
Parameter SI-4 (19)-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-4 (19) What is the solution and how is it implemented?

SI-4 (20) CONTROL ENHANCEMENT (H)

The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.

SI-4 (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	

SI-4 (20) What is the solution and how is it implemented?

SI-4 (22) CONTROL ENHANCEMENT (H)

The information system detects network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts* [*Assignment: organization-defined personnel or roles*]].

SI-4 (22)	Control Summary Information
Responsible Role:	
Parameter SI-4 (22)-1:	
Parameter SI-4 (22)-2:	

SI-4 (22)	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	

SI-4 (22) 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-4 (24) CONTROL ENHANCEMENT (H)

The information system discovers, collects, distributes, and uses indicators of compromise.

SI-4 (24)	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 (24) 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;

(b) Generates internal security alerts, advisories, and directives as deemed necessary;

(c) Disseminates security alerts, advisories, and directives to [*FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities*]; and

(d) Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

SI-5	Control Summary Information
Responsible Role:	
Parameter SI-5(a):	
Parameter SI-5(c):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing 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-5 (1) CONTROL ENHANCEMENT (H)

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

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

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

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

SI-6 What is the solution and how is it implemented?	
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) ☐ 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 (2) CONTROL ENHANCEMENT (H)

The organization employs automated tools that provide notification to [*Assignment: organization-defined personnel or roles]*] upon discovering discrepancies during integrity verification.

SI-7 (2)	Control Summary Information
Responsible Role:	
Parameter SI-7 (2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

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

SI-7 (5) CONTROL ENHANCEMENT (H)

The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements* [*Assignment: organization-defined security safeguard*]] when integrity violations are discovered.

SI-7 (5)	Control Summary Information
Responsible Role:	
Parameter SI-7 (5):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

SI-7 (5)	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	

SI-7 (5) 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-7 (14) CONTROL ENHANCEMENT (H)

The organization:

(a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

(b) Provides exceptions to the source code requirement only for compelling mission/ operational requirements and with the approval of the authorizing official.

SI-7 (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-7 (14) 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 ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (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	

SI-8 (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	

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

SI-12	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-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)	

SI-16	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	

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
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 an Information Security Policies and Procedures 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 Information System Name (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.	Hope Health Care Information System	HHCIS

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

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	1. Does the ISA collect, maintain, or share PII in any identifiable form?
Select One	2. Does the ISA collect, maintain, or share PII information from or about the public?
Select One	3. Has a Privacy Impact Assessment ever been performed for the ISA?
Select One	4. 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

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 Health Care Information System has been determined to have a security categorization of Choose level.

Hope Health Care Information System (HHCIS) is a general information system for small and medium-sized hospitals. It covers the main management functions of hospitals and the main links of patients in hospitals.

HHCIS is not simply a software, it is a result of the perfect unification of the hospital's management thinking, the hospital's business experience of various departments and the latest computer technology.

This system can bring convenient and fast services to patients, promote standardized management of hospitals, and greatly reduce medical errors.

Methodology

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.

The Table 15- 9 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
Access to Care	Low	Moderate	Low	Low	Moderate	Moderate	Impaired access availability may cause adverse effect on agency operations and agency assets
Population Health Management and Consumer Safety	Low	Moderate	Low	Low	Moderate	Low	N/A
Health Care Administration	Low	Moderate	Low	High	Moderate	Low	Health Care Administration has sensitive information related to employees, such as bank card number, mobile phone number, etc
Health Care Delivery Services	Low	High	Low	High	High	Low	Health Care Delivery Services include patient's sensitive

Information Type	NIST SP 800-60 V2 RI Recommended Confidentiality Impact Level	NIST SP 800-60 V2 RI Recommended Integrity Impact Level	NIST SP 800-60 V2 RI Recommended Availability Impact Level	CSP Selected Confidentiality Impact Level	CSP Selected Integrity Impact Level	CSP Selected Availability Impact Level	Statement for Impact Adjustment Justification
							information, such as ID card, etc. The patient's medical records cannot be disclosed.
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.