

Office of Inspector General

ASW Customer SSP

|  |
| --- |
| ***FedRAMP Model Template*** |

***December 13, 2016***

**Prepared by:**

Lunarline Inc.



[This Page intentionally Left Blank]

Introduction

This template is designed to help AWS customers write a System Security Plan (SSP) that describes an application built upon AWS services. A completed SSP can be used as the basis for a FedRAMP or an agency-specific authorization effort. This template is pre-populated with instructions and guidance on how to complete each section. It follows the AWS shared responsibility model, clearlyx defining which controls are the responsibility of AWS and which are managed by the customer.

**\*\*Please Note:** This AWS Customer SSP Template covers all of the controls required for a FedRAMP High impact level system. For FedRAMP Moderate and Low impact systems, the controls from the higher baselines should be removed and the relative parameters for the remaining controls updated to the appropriate level (Moderate or Low). \*\*

For a listing of all authorized AWS Services please visit <https://aws.amazon.com/compliance/fedramp>. Additionally, for a listing of all FedRAMP services-in-scope please visit <https://aws.amazon.com/compliance/services-in-scope/>. It is the responsibility of the customer to make a **risk-based decision** prior to leveraging FedRAMP compliant AWS Services.

AWS also provides additional materials that can assist with the design of a secure architecture. These whitepapers are available on the AWS website (aws.amazon.com/whitepapers/) for further security details refer to:

* *AWS Security Best Practices* 
  + ***Important Note:*** *Please review the “services-in-scope” URL provided above to determine FedRAMP authorized AWS Services prior to their use. This whitepaper is a “best practice” and potentially includes AWS Services that are not in-scope for FedRAMP.)*
* *Amazon Web Services: Overview of Security Processes*

A brief discussion about shared responsibility follows. We have also included an instruction guide that describes the steps required to complete your SSP. The instruction sections, pages 1-8 of this document, should be removed before the final SSP is published.

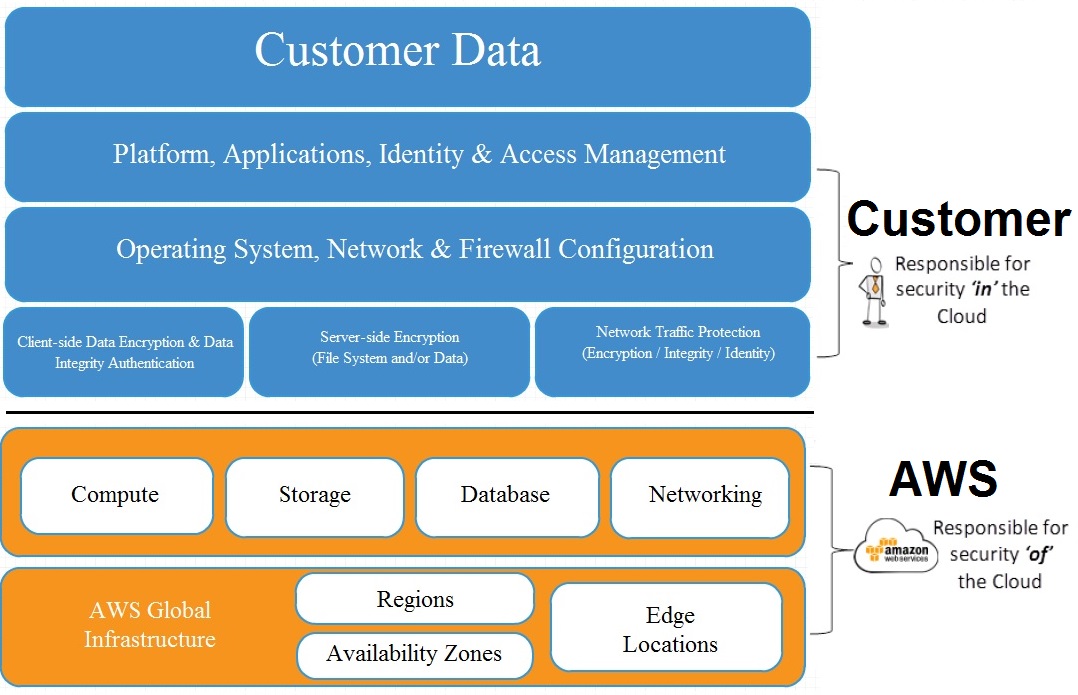
Disclaimer

*THIS DOCUMENT IS © 2010-2016 AMAZON.COM, INC., OR ITS AFFILIATES (“AMAZON”) AND CONSTITUTES AMAZON CONFIDENTIAL INFORMATION.  THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT AMAZON WEB SERVICES, INC.’s (“AWS”) PRIOR WRITTEN CONSENT. This document is for information purposes only. It represents AWS’s current product offerings as of the date of issue of this document.  Partners and their customers are responsible for making their own independent assessment of the information in this document and any use of AWS products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Amazon, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its partners and customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its partners and customers.  Partner agrees that it will include a disclaimer similar to the foregoing in any document based on the contents of this document.*

Shared Responsibility Guidance

Control Responsibilities

AWS cloud services provide the infrastructure to support customer workloads. Regions, Availability Zones (AZs), and services comprise the General Support System (GSS) that supports each customer’s Major Application (MA).



1. Control Responsibilities

AWS Responsibilities

Applications built on top of the AWS infrastructure inherit the features and configurable options provided by AWS. In this model, AWS provides the service delivery layers including infrastructure and service management processes. AWS manages the cloud infrastructure including the network, data storage, system resources, data centers, physical security, reliability, and supporting hardware and software.

Customer Responsibilities

The customer is responsible for their guest operating systems, deployed applications, and limited configuration control of select networking resources (e.g., firewalls) but is not responsible for the underlying cloud infrastructure. At customer instantiation of a host, AWS makes no warranties as to the patch level or configuration settings included with that host. Customer responsibility includes updating any instance to a patch level that is acceptable by the customer organization and choosing configurations to suit their specific needs. Upon deployment of virtual machines, the customer assumes full administrator access and is responsible for performing all configuration, patching, security hardening, vulnerability scanning and application installation, as necessary.

Service Instance Management

Customers are responsible for managing their instantiations of storage buckets and objects, compute instances and Virtual Private Cloud (VPC) network environments. This includes customer-installed operating systems and applications. Customers are also responsible for managing specific controls relating to shared touch points within the security authorization boundary such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing VPC network configurations.

Customers provision and configure their implementation of storage, virtual machines and VPC using API calls to the AWS API endpoints. This allows the customer to launch and terminate cloud instances, change firewall parameters, and perform other management functions.

Application Management

Major Applications (MAs) that run on AWS are entirely the responsibility of each customer to configure and maintain. This System Security Plan template addresses the controls relevant to each application.

Guest Operating System Maintenance

AWS provided images (Amazon Linux AMIs) for the guest operating system are patched to a point in time. The installation will be the minimum installation of the operating system. AMIs are also available that contain standard releases from OS vendors such as Windows Server, RHEL, SUSE Linux and Ubuntu Linux with no additional configuration or patching applied to the image.

AWS does not perform patch management, system hardening, and does not provide any application support within the customer environment.

Upon the customer instantiation of an AMI, AWS makes no warranties as to the patch level or configuration settings. Customer responsibility includes updating any instance to an acceptable patch level and configuring it to suit specific needs. Upon deployment of virtual machines, the customer assumes full administrator access and is responsible for performing additional configuration, patching, security hardening, vulnerability scanning and application installation, as necessary. AWS does not have administrator access to customer’s AMIs.

Shared Responsibilities

Because customers are building systems on top of the AWS cloud infrastructure, many security measures will be *shared*: customers will provide security for their software components and AWS will provide security for its infrastructure. In other cases, customers will be able to *inherit* the security controls from AWS, meaning customers won’t have to provide those controls for their components because AWS is already providing it. Control responsibilities are described in this document, or listed in a more concise form in the AWS FedRAMP Control Implementation Summary (CIS).

Instructions

Follow the below instructions to complete all sections of the SSP, additional guidance is provided throughout this SSP template:

|  |  |
| --- | --- |
| **Section 1:** | * Populate the "Information System Name" * Populate the "Information System Abbreviation" * Populate the "Unique Identifier". This unique identifier and system abbreviation will be provided to you during the initiation process by the FedRAMP PMO. |
| **Section 2:** | * First complete sub-sections 2.1 and 2.2, the impact levels for the Confidentiality, Integrity, and Availability objectives. Refer to FIPS 199, Standards for Security Categorization of Federal Information and Information Systems for additional guidance on choosing these levels. * Next, check the appropriate box that corresponds to your overall impact categorization in Table 2-1. Remember that the highest rating from any one category becomes the information system's overall security categorization. * Complete the E-authentication questions in Section 2.3. Refer to the e-Authentication Template located on the FedRAMP website for additional guidance. |
| **Section 3:** | * Enter contact information for the system owner in this section. |
| **Section 4:** | * Follow the instruction and determine the path that the CSP is using to obtain an authorization. |
| **Section 5:** | * Enter contact information for the other designated contacts in this section. |
| **Section 6:** | * Enter contact information for your ISSO or other security representative, and the FedRAMP appointed ISSO (which is not applicable if using the Agency FedRAMP model). |
| **Section 7:** | * Check the appropriate box that corresponds to the current operational status. |
| **Section 8:** | * Fill in the application name, following the search/replace guide above. In Section 8.1, check the service layers that apply to this SSP. * In 8.2, check the cloud deployment model that applies. * In 8.3, enter the names of any other provisional authorizations that are leveraged as part of your authorization boundary. Include the appropriate AWS system, following the search/replace guide below. |
| **Section 9:** | * Fill in this section with a complete description of the application. There are additional instructions about each subsection within the body of the document. |
| **Section 10:** | * Complete each subsection based on the instructions listed within brackets. |
| **Section 11:** | * List any system interconnections, if applicable, according to the guidance within the body of the text. |
| **Sections 12:** | * Refer to FedRAMP.gov for a template on the laws, regulations, standards, and guidance. Leverage this template to populate tables 12-1 and 12-2 of this SSP. This is also within Section 15.12 of this document. |
| **Section 13:** | * Throughout this section populate the following in each control, as applicable:   + "Responsible Role" marked with "[TBD by Customer]".   + "Parameters" marked with "[TBD by Customer]". These parameters need to be determined by the customer leveraging this SSP.   + "Implementation Status" which needs to be determined by the customer.   + “Implementation Statement” (Labeled as “What is the solution and how is it implemented?”)     - Work to document the customer implementation marked with brackets "[ ]". Italicized guidance has been provided by AWS regarding customer responsibility and should be removed/replaced by the customer with system-specific information. |
| **Section 14:** | * N/A |
| **Section 15:** | * Fill out the necessary supporting documentation within this section. |

Search and Replace Instructions

To simplify data entry and reduce copy/paste efforts throughout the SSP, some recurring 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 the fields in the table below with brackets surrounding the text “[ ]”, search and replace all instances (including the brackets) based on the guidance below:

**\*\*Please Note: Do not do a global replace for “[TBD by Customer]” - This value will depend on whether this is a role, parameter, or implementation statement and must be determined by the customer. \*\***

|  |  |
| --- | --- |
| **Repeatable Field** | **Replace with** |
| CSP Name | Your company name (This is a global replace) |
| Information System Name | The name of your system or application (This is a global replace) |
| Information System Abbreviation | The abbreviated name of your system or application (This is a global replace) |
| Version [Number] | The version number of your document. (This is a global replace) |
| [Date] | Date the document was updated/created. (This is a global replace) |
| [TBD by Customer] | This is the customer’s responsibility to determine and obtain this information.  **Do not do a global replace for this value** as this may depend on whether this is a role, parameter, or implementation statement throughout the document and must be determined by the customer. |
| [AWS Region] | **Search and replace all -** This will either be “US East/West” or “AWS GovCloud (US)” and is dependent on the AWS region being leveraged by the customer. Please visit www.FedRAMP.gov regarding the different AWS regions that are authorized. |
| [Date of Authorization] | **Search and replace all** – This is the AWS Authorization Date and is dependent on the AWS region being leveraged by the customer. Please visit www.FedRAMP.gov’s marketplace for the most up-to-date information regarding AWS’ authorization dates. |
| [Provisional OR Agency] | **Search and replace all** – This will either be an “Agency” or a “Provisional” ATO depending on the AWS region being leveraged by the customer. |

Guidance on Control Headings

The security controls are contained in Section 13. The control headings are exact copies of those from the FedRAMP SSP template, and so should not be modified. Control parameters and definitions, which appear as [*Assignment: organization-defined variable*], should be defined in the control description below each heading according to the customer’s specific requirements.

See the Shared Responsibility Guidance section for a discussion of which controls apply to the AWS infrastructure, the application, or are shared between the two.

Control Descriptions

The control descriptions are pre-populated with guidance or instructions in *[brackets].* Replace these paragraphs with your own text as applicable.

Control implementation statements should be concise, but completely address each point in the control requirements. A general best practice is to answer who, what, when, where, and how often. These are the types of details that assessors will look for in the SSP, and will measure against during a formal FedRAMP assessment. If the control is not fully implemented currently, mark it as partially implemented and be sure to document any mitigating controls that would reduce the level of residual risk.

If the control has a shared responsibility between AWS and the customer application, there will be two parts to each description. One for the implementation of your application (labeled Application), and the other is for the AWS responsibility (labeled Infrastructure). Any statements about inheritance or reference, which are not in brackets, should remain.

Federal agencies may request a copy of the AWS SSP, included in the AWS FedRAMP package, in order to review the implementation details of controls from the AWS perspective for making their ATO determination. Remember that the application SSP should not duplicate the descriptions in the AWS SSP, but instead should describe controls from the application’s perspective.

Once the controls have been fully described, remove all of these instructions from the final document.

Final Note

This SSP template is a resource for AWS customers and is meant to be used for AWS-based application Assessment and Authorization (A&A) packages to document to compliance posture of their applications and systems built on AWS. Separate from the AWS FedRAMP package, each major application built upon AWS will have its own SSP, third-party assessment, FedRAMP documentation package, and ATO decision. Customers are encouraged to contact an AWS Solutions Architect (SA) or the AWS Compliance team for additional help with this process and to provide feedback on this template (awscompliance@amazon.com).

As always, a great resource to leverage for training and/or additional FedRAMP guidance and information can be found at www.FedRAMP.gov.

***Remove this line and everything above it***



Office of Inspector General

FedRAMP System Security Plan (SSP)  
High Baseline

|  |
| --- |
| ***CSP Name***  ***Information System Name***  ***Version [Number]*** |

***December 13, 2016***

Document Change Control Sheet

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **File Name** | **Initials** | **Status/Comments** | **Version** |
| xx/02/2016 | [Information System Name].docx | TF | Initial document preparation | 1.0 |
| xx/05/2016 | [Information System Name].docx | GO | Quality Review | 1.0 |
| 11/XX/2016 | [Information System Name].docx | GO | Reviewed and forwarded to the COR | 1.0 |

***Note: Retain this table for document maintenance.***

**TF** – Tiffany Foxworth

**GO** – George Oyedele

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> |

**Table of Contents**

[1 Information System Name/Title 21](#_Toc468804729)

[2 Information System Categorization 21](#_Toc468804730)

[2.1 Information Types 21](#_Toc468804731)

[2.2 Security Objectives Categorization (FIPS 199) 23](#_Toc468804732)

[2.3 E-Authentication Determination 24](#_Toc468804733)

[3 Information System Owner 25](#_Toc468804734)

[4 Authorizing Official 25](#_Toc468804735)

[5 Other Designated Contacts 25](#_Toc468804736)

[6 Assignment of Security Responsibility 26](#_Toc468804737)

[7 Information System Operational Status 27](#_Toc468804738)

[8 Information System Type 28](#_Toc468804739)

[8.1 Cloud Service Models 28](#_Toc468804740)

[8.2 Cloud Deployment Models 29](#_Toc468804741)

[8.3 Leveraged Authorizations 29](#_Toc468804742)

[9 General System Description 30](#_Toc468804743)

[9.1 System Function or Purpose 30](#_Toc468804744)

[9.2 Information System Components and Boundaries 30](#_Toc468804745)

[9.3 Types of Users 31](#_Toc468804746)

[9.4 Network Architecture 32](#_Toc468804747)

[10 System Environment 33](#_Toc468804748)

[10.1 Hardware Inventory 33](#_Toc468804749)

[10.2 Software Inventory 33](#_Toc468804750)

[10.3 Network Inventory 33](#_Toc468804751)

[10.4 Data Flow 34](#_Toc468804752)

[10.5 Ports, Protocols and Services 34](#_Toc468804753)

[11 System Interconnections 35](#_Toc468804754)

[12 Laws, Regulations, Standards, and Guidance 37](#_Toc468804755)

[12.1 Applicable Laws and Regulations 37](#_Toc468804756)

[12.2 APPLICABLE STANDARDS AND GUIDANCE 37](#_Toc468804757)

[13 Minimum Security Controls 37](#_Toc468804758)

[13.1 Access Control (AC) 47](#_Toc468804759)

[AC-1 Access Control Policy and Procedures Requirements 47](#_Toc468804760)

[AC-2 Account Management 49](#_Toc468804761)

[AC-2 (1) Control Enhancement 55](#_Toc468804762)

[AC-2 (2) Control Enhancement 55](#_Toc468804763)

[AC-2 (3) Control Enhancement 56](#_Toc468804764)

[AC-2 (4) Control Enhancement 57](#_Toc468804765)

[AC-2 (5) Control Enhancement 58](#_Toc468804766)

[AC-2 (7) Control Enhancement 59](#_Toc468804767)

[AC-2 (9) Control Enhancement 61](#_Toc468804768)

[AC-2 (10) Control Enhancement 62](#_Toc468804769)

[AC-2 (11) Control Enhancement 63](#_Toc468804770)

[AC-2 (12) Control Enhancement 64](#_Toc468804771)

[AC-3 Access Enforcement 66](#_Toc468804772)

[AC-4 Information Flow Enforcement 66](#_Toc468804773)

[AC-4 (21) Control Enhancement 67](#_Toc468804774)

[AC-5 Separation of Duties 68](#_Toc468804775)

[AC-6 Least Privilege 69](#_Toc468804776)

[AC-6 (1) Control Enhancement 70](#_Toc468804777)

[AC-6 (2) Control Enhancement 71](#_Toc468804778)

[AC 6 (5) Control Enhancement 72](#_Toc468804779)

[AC-6 (9) Control Enhancement 73](#_Toc468804780)

[AC-6 (10) Control Enhancement 74](#_Toc468804781)

[AC-7 Unsuccessful Login Attempts 74](#_Toc468804782)

[AC-8 System Use Notification 75](#_Toc468804783)

[AC-10 Concurrent Session Control 79](#_Toc468804784)

[AC-11 Session Lock 80](#_Toc468804785)

[AC-11 (1) Control Enhancement 81](#_Toc468804786)

[AC-12 Session Termination 82](#_Toc468804787)

[AC-14 Permitted Actions without Identification or Authentication 83](#_Toc468804788)

[AC-17 Remote Access 84](#_Toc468804789)

[AC-17 (1) Control Enhancement 85](#_Toc468804790)

[AC-17 (2) Control Enhancement 86](#_Toc468804791)

[AC-17 (3) Control Enhancement 87](#_Toc468804792)

[AC-17 (4) Control Enhancement 87](#_Toc468804793)

[AC-17 (9) Control Enhancement 88](#_Toc468804794)

[AC-18 Wireless Access 89](#_Toc468804795)

[AC-18 (1) Control Enhancement 90](#_Toc468804796)

[AC-19 Access Control for Mobile Devices 91](#_Toc468804797)

[AC-19 (5) Control Enhancement 92](#_Toc468804798)

[AC-20 Use of External Information Systems 93](#_Toc468804799)

[AC-20 (1) Control Enhancement 94](#_Toc468804800)

[AC-20 (2) Control Enhancement 95](#_Toc468804801)

[AC-21 Information Sharing 96](#_Toc468804802)

[AC-22 Publicly Accessible Content 97](#_Toc468804803)

[13.2 Awareness and Training (AT) 98](#_Toc468804804)

[AT-1 Security Awareness and Training Policy and Procedures 98](#_Toc468804805)

[AT-2 Security Awareness 100](#_Toc468804806)

[AT-2 (2) Control Enhancement 101](#_Toc468804807)

[AT-3 Role-Based Security Training 102](#_Toc468804808)

[AT-4 Security Training Records 103](#_Toc468804809)

[13.3 Audit and Accountability (AU) 104](#_Toc468804810)

[AU-1 Audit and Accountability Policy and Procedures 104](#_Toc468804811)

[AU-2 Audit Events 105](#_Toc468804812)

[AU-2 (3) Control Enhancement 107](#_Toc468804813)

[AU-3 Content of Audit Records 108](#_Toc468804814)

[AU-3 (1) Control Enhancement 109](#_Toc468804815)

[AU-4 Audit Storage Capacity 110](#_Toc468804816)

[AU-5 Response to Audit Processing Failures 111](#_Toc468804817)

[AU-6 Audit Review, Analysis, and Reporting 112](#_Toc468804818)

[AU-6 (1) Control Enhancement 113](#_Toc468804819)

[AU-6 (3) Control Enhancement 114](#_Toc468804820)

[AU-7 Audit Reduction and Report Generation 115](#_Toc468804821)

[AU-7 (1) Control Enhancement 116](#_Toc468804822)

[AU-8 Time Stamps 117](#_Toc468804823)

[AU-8 (1) Control Enhancement 118](#_Toc468804824)

[AU-9 Protection of Audit Information 121](#_Toc468804825)

[AU-9 (2) Control Enhancement 121](#_Toc468804826)

[AU-9 (4) Control Enhancement 122](#_Toc468804827)

[AU-11 Audit Record Retention 123](#_Toc468804828)

[AU-12 Audit Generation 124](#_Toc468804829)

[13.4 Security Assessment and Authorization (CA) 125](#_Toc468804830)

[CA-1 Security Assessment and Authorization Policy and Procedures 125](#_Toc468804831)

[CA-2 Security Assessments 127](#_Toc468804832)

[CA-2 (1) Control Enhancement 128](#_Toc468804833)

[CA-2 (2) Control Enhancement 129](#_Toc468804834)

[CA-2 (3) Control Enhancement 130](#_Toc468804835)

[CA-3 System Interconnections 131](#_Toc468804836)

[CA-3 (3) Control Enhancement 133](#_Toc468804837)

[CA-3 (5) Control Enhancement 134](#_Toc468804838)

[CA-5 Plan of Action and Milestones 135](#_Toc468804839)

[CA-6 Security Authorization 136](#_Toc468804840)

[CA-7 Continuous Monitoring 138](#_Toc468804841)

[CA-7 (1) Control Enhancement 142](#_Toc468804842)

[CA-8 Penetration Testing 143](#_Toc468804843)

[CA-8 (1) Control Enhancement 144](#_Toc468804844)

[CA-9 Internal System Connections 145](#_Toc468804845)

[13.5 Configuration Management (CM) 146](#_Toc468804846)

[CM-1 Configuration Management Policies and Procedures 146](#_Toc468804847)

[CM-2 Baseline Configuration 147](#_Toc468804848)

[CM-2 (1) Control Enhancement 148](#_Toc468804849)

[CM-2 (2) Control Enhancement 149](#_Toc468804850)

[CM-2 (3) Control Enhancement 150](#_Toc468804851)

[CM-2 (7) Control Enhancement 151](#_Toc468804852)

[CM-3 Configuration Change Control 152](#_Toc468804853)

[CM-4 Security Impact Analysis 155](#_Toc468804854)

[CM-5 Access Restrictions for Change 156](#_Toc468804855)

[CM-5 (1) Control Enhancement 156](#_Toc468804856)

[CM-5 (3) Control Enhancement 157](#_Toc468804857)

[CM-5 (5) Control Enhancement 158](#_Toc468804858)

[CM-6 Configuration Settings 159](#_Toc468804859)

[CM-6 (1) Control Enhancement 161](#_Toc468804860)

[CM-7 Least Functionality 162](#_Toc468804861)

[CM-7 (1) Control Enhancement 163](#_Toc468804862)

[CM-7 (2) Control Enhancement 164](#_Toc468804863)

[CM-7 (5) Control Enhancement 165](#_Toc468804864)

[CM-8 Information System Component Inventory 167](#_Toc468804865)

[CM-8 (1) Control Enhancement 168](#_Toc468804866)

[CM-8 (3) Control Enhancement 169](#_Toc468804867)

[CM-8 (5) Control Enhancement 171](#_Toc468804868)

[CM-9 Configuration Management Plan 172](#_Toc468804869)

[CM-10 Software Usage Restrictions 173](#_Toc468804870)

[CM-10 (1) Control Enhancement 175](#_Toc468804871)

[CM-11 User-Installed Software 175](#_Toc468804872)

[13.6 Contingency Planning (CP) 177](#_Toc468804873)

[CP-1 Contingency Planning Policy and Procedures 177](#_Toc468804874)

[CP-2 Contingency Plan 178](#_Toc468804875)

[CP-2 (1) Control Enhancement 181](#_Toc468804876)

[CP-2 (2) Control Enhancement 182](#_Toc468804877)

[CP-2 (3) Control Enhancement 182](#_Toc468804878)

[CP-2 (8) Control Enhancement 183](#_Toc468804879)

[CP-3 Contingency Training 184](#_Toc468804880)

[CP-4 Contingency Plan Testing 185](#_Toc468804881)

[CP-4 (1) Control Enhancement 186](#_Toc468804882)

[CP-6 Alternate Storage Site 187](#_Toc468804883)

[CP-6 (1) Control Enhancement 188](#_Toc468804884)

[CP-6 (3) Control Enhancement 189](#_Toc468804885)

[CP-7 Alternate Processing Site 190](#_Toc468804886)

[CP-7 (1) Control Enhancement 191](#_Toc468804887)

[CP-7 (2) Control Enhancement 192](#_Toc468804888)

[CP-7 (3) Control Enhancement 193](#_Toc468804889)

[CP-8 Telecommunications Services 194](#_Toc468804890)

[CP-8 (1) Control Enhancement 195](#_Toc468804891)

[CP-8 (2) Control Enhancement 196](#_Toc468804892)

[CP-9 Information System Backup 197](#_Toc468804893)

[CP-9 (1) Control Enhancement 199](#_Toc468804894)

[CP-9 (3) Control Enhancement 200](#_Toc468804895)

[CP-10 Information System Recovery and Reconstitution 201](#_Toc468804896)

[CP-10 (2) Control Enhancement 202](#_Toc468804897)

[13.7 Identification and Authentication (IA) 203](#_Toc468804898)

[IA-1 Identification and Authentication Policy and Procedures 203](#_Toc468804899)

[IA-2 Identification and Authentication (Organizational Users) 204](#_Toc468804900)

[IA-2 (1) Control Enhancement 205](#_Toc468804901)

[IA-2 (2) Control Enhancement 206](#_Toc468804902)

[IA-2 (3) Control Enhancement 206](#_Toc468804903)

[IA-2 (5) Control Enhancement 207](#_Toc468804904)

[IA-2 (8) Control Enhancement 208](#_Toc468804905)

[IA-2 (11) Control Enhancement 209](#_Toc468804906)

[IA-2 (12) Control Enhancement 210](#_Toc468804907)

[IA-3 Device Identification and Authentication 211](#_Toc468804908)

[IA-4 Identifier Management 211](#_Toc468804909)

[IA-4 (4) Control Enhancement 214](#_Toc468804910)

[IA-5 Authenticator Management 215](#_Toc468804911)

[IA-5 (1) Control Enhancement 219](#_Toc468804912)

[IA-5 (2) Control Enhancement 222](#_Toc468804913)

[IA-5 (3) Control Enhancement 223](#_Toc468804914)

[IA-5 (4) Control Enhancement 224](#_Toc468804915)

[IA-5 (6) Control Enhancement 225](#_Toc468804916)

[IA-5 (7) Control Enhancement 226](#_Toc468804917)

[IA-5 (11) Control Enhancement 227](#_Toc468804918)

[IA-6 Authenticator Feedback 228](#_Toc468804919)

[IA-7 Cryptographic Module Authentication 228](#_Toc468804920)

[IA-8 Identification and Authentication (Non-Organizational Users) 229](#_Toc468804921)

[IA-8 (1) Control Enhancement 230](#_Toc468804922)

[IA-8 (2) Control Enhancement 231](#_Toc468804923)

[IA-8 (3) Control Enhancement 231](#_Toc468804924)

[IA-8 (4) Control Enhancement 232](#_Toc468804925)

[13.8 Incident Response (IR) 233](#_Toc468804926)

[IR-1 Incident Response Policy and Procedures 233](#_Toc468804927)

[IR-2 Incident Response Training 234](#_Toc468804928)

[IR-3 Incident Response Testing 235](#_Toc468804929)

[IR-3 (2) Control Enhancement 236](#_Toc468804930)

[IR-4 Incident Handling 237](#_Toc468804931)

[IR-4 (1) Control Enhancement 239](#_Toc468804932)

[IR-5 Incident Monitoring 240](#_Toc468804933)

[IR-6 Incident Reporting 241](#_Toc468804934)

[IR-6 (1) Control Enhancement 242](#_Toc468804935)

[IR-7 Incident Response Assistance 243](#_Toc468804936)

[IR-7 (1) Control Enhancement 244](#_Toc468804937)

[IR-7 (2) Control Enhancement 244](#_Toc468804938)

[IR-8 Incident Response Plan 245](#_Toc468804939)

[IR-9 Information Spillage Response 249](#_Toc468804940)

[IR-9 (1) Control Enhancement 252](#_Toc468804941)

[IR-9 (2) Control Enhancement 253](#_Toc468804942)

[IR-9 (3) Control Enhancement 253](#_Toc468804943)

[IR-9 (4) Control Enhancement 254](#_Toc468804944)

[13.9 Maintenance (MA) 255](#_Toc468804945)

[MA-1 System Maintenance Policy and Procedures 255](#_Toc468804946)

[MA-2 Controlled Maintenance 257](#_Toc468804947)

[MA-3 Maintenance Tools 258](#_Toc468804948)

[MA-3 (1) Control Enhancement 259](#_Toc468804949)

[MA-3 (2) Control Enhancement 259](#_Toc468804950)

[MA-3 (3) Control Enhancement 260](#_Toc468804951)

[MA-4 Nonlocal Maintenance 261](#_Toc468804952)

[MA-4 (2) Control Enhancement 262](#_Toc468804953)

[MA-5 Maintenance Personnel 263](#_Toc468804954)

[MA-5 (1) Control Enhancement 264](#_Toc468804955)

[MA-6 Timely Maintenance 265](#_Toc468804956)

[13.10 Media Protection (MP) 266](#_Toc468804957)

[MP-1 Media Protection Policy and Procedures 266](#_Toc468804958)

[MP-2 Media Access 267](#_Toc468804959)

[MP-3 Media Marking 268](#_Toc468804960)

[MP-4 Media Storage 269](#_Toc468804961)

[MP-5 Media Transport 270](#_Toc468804962)

[MP-5 (4) Control Enhancement 271](#_Toc468804963)

[MP-6 Media Sanitization 272](#_Toc468804964)

[MP-6 (2) Control Enhancement 273](#_Toc468804965)

[MP-7 Media Use 273](#_Toc468804966)

[MP-7 (1) Control Enhancement 274](#_Toc468804967)

[13.11 Physical and Environmental Protection (PE) 275](#_Toc468804968)

[PE-1 Physical and Environmental Protection Policy and Procedures 275](#_Toc468804969)

[PE-2 Physical Access Authorizations 276](#_Toc468804970)

[PE-3 Physical Access Control 277](#_Toc468804971)

[PE-4 Access Control for Transmission Medium 279](#_Toc468804972)

[PE-5 Access Control for Output Devices 280](#_Toc468804973)

[PE-6 Monitoring Physical Access 280](#_Toc468804974)

[PE-6 (1) Control Enhancement 281](#_Toc468804975)

[PE-8 Visitor Access Records 282](#_Toc468804976)

[PE-9 Power Equipment and Cabling 283](#_Toc468804977)

[PE-10 Emergency Shutoff 284](#_Toc468804978)

[PE-11 Emergency Power 284](#_Toc468804979)

[PE-12 Emergency Lighting 285](#_Toc468804980)

[PE-13 Fire Protection 286](#_Toc468804981)

[PE-13 (2) Control Enhancement 287](#_Toc468804982)

[PE-13 (3) Control Enhancement 287](#_Toc468804983)

[PE-14 Temperature and Humidity Controls 288](#_Toc468804984)

[PE-14 (2) Control Enhancement 289](#_Toc468804985)

[PE-15 Water Damage Protection 290](#_Toc468804986)

[PE-16 Delivery and Removal 290](#_Toc468804987)

[PE-17 Alternate Work Site 291](#_Toc468804988)

[13.12 Planning (PL) 292](#_Toc468804989)

[PL-1 Security Planning Policy and Procedures 292](#_Toc468804990)

[PL-2 System Security Plan 293](#_Toc468804991)

[PL-2 (3) Control Enhancement 295](#_Toc468804992)

[PL-4 Rules of Behavior 296](#_Toc468804993)

[PL-4 (1) Control Enhancement 298](#_Toc468804994)

[PL-8 Information Security Architecture 299](#_Toc468804995)

[13.13 Personnel Security (PS) 301](#_Toc468804996)

[PS-1 Personnel Security Policy and Procedures 301](#_Toc468804997)

[PS-2 Position Risk Designation 302](#_Toc468804998)

[PS-3 Personnel Screening 303](#_Toc468804999)

[PS-3 (3) Control Enhancement 304](#_Toc468805000)

[PS-4 Personnel Termination 305](#_Toc468805001)

[PS-5 Personnel Transfer 308](#_Toc468805002)

[PS-6 Access Agreements 309](#_Toc468805003)

[PS-7 Third-Party Personnel Security 311](#_Toc468805004)

[PS-8 Personnel Sanctions 312](#_Toc468805005)

[13.14 Risk Assessment (RA) 314](#_Toc468805006)

[RA-1 Risk Assessment Policy and Procedures 314](#_Toc468805007)

[RA-2 Security Categorization 315](#_Toc468805008)

[RA-3 Risk Assessment 316](#_Toc468805009)

[RA-5 Vulnerability Scanning 318](#_Toc468805010)

[RA-5 (1) Control Enhancement 322](#_Toc468805011)

[RA-5 (2) Control Enhancement 322](#_Toc468805012)

[RA-5 (3) Control Enhancement 323](#_Toc468805013)

[RA-5 (5) Control Enhancement 324](#_Toc468805014)

[RA-5 (6) Control Enhancement 325](#_Toc468805015)

[RA-5 (8) Control Enhancement 326](#_Toc468805016)

[13.15 System and Services Acquisition (SA) 327](#_Toc468805017)

[SA-1 System and Services Acquisition Policy and Procedures 327](#_Toc468805018)

[SA-2 Allocation of Resources 328](#_Toc468805019)

[SA-3 System Development Life Cycle 329](#_Toc468805020)

[SA-4 Acquisition Process 331](#_Toc468805021)

[SA-4 (1) Control Enhancement 334](#_Toc468805022)

[SA-4 (2) Control Enhancement 335](#_Toc468805023)

[SA-4 (8) Control Enhancement 336](#_Toc468805024)

[SA-4 (9) Control Enhancement 337](#_Toc468805025)

[SA-4 (10) Control Enhancement 337](#_Toc468805026)

[SA-5 Information System Documentation 338](#_Toc468805027)

[SA-8 Security Engineering Principles 341](#_Toc468805028)

[SA-9 External Information System Services 341](#_Toc468805029)

[SA-9 (1) Control Enhancement 343](#_Toc468805030)

[SA-9 (2) Control Enhancement 344](#_Toc468805031)

[SA-9 (4) Control Enhancement 345](#_Toc468805032)

[SA-9 (5) Control Enhancement 346](#_Toc468805033)

[SA-10 Developer Configuration Management 347](#_Toc468805034)

[SA-10 (1) Control Enhancement 349](#_Toc468805035)

[SA-11 Developer Security Testing and Evaluation 350](#_Toc468805036)

[SA-11 (1) Control Enhancement 352](#_Toc468805037)

[SA-11 (2) Control Enhancement 353](#_Toc468805038)

[SA-11 (8) Control Enhancement 354](#_Toc468805039)

[13.16 System and Communications Protection (SC) 355](#_Toc468805040)

[SC-1 System and Communications Protection Policy and Procedures 355](#_Toc468805041)

[SC-2 Application Partitioning 356](#_Toc468805042)

[SC-4 Information in Shared Resources 357](#_Toc468805043)

[SC-5 Denial of Service Protection 358](#_Toc468805044)

[SC-6 Resource Availability 359](#_Toc468805045)

[SC-7 Boundary Protection 360](#_Toc468805046)

[SC-7 (3) Control Enhancement 361](#_Toc468805047)

[SC-7 (4) Control Enhancement 362](#_Toc468805048)

[SC-7 (5) Control Enhancement 364](#_Toc468805049)

[SC-7 (7) Control Enhancement 365](#_Toc468805050)

[SC-7 (8) Control Enhancement 366](#_Toc468805051)

[SC-7 (12) Control Enhancement 367](#_Toc468805052)

[SC-7 (13) Control Enhancement 368](#_Toc468805053)

[SC-7 (18) Control Enhancement 369](#_Toc468805054)

[SC-8 Transmission Confidentiality and Integrity 370](#_Toc468805055)

[SC-8 (1) Control Enhancement 371](#_Toc468805056)

[SC-10 Network Disconnect 371](#_Toc468805057)

[SC-12 Cryptographic Key Establishment and Management 372](#_Toc468805058)

[SC-12 (2) Control Enhancement 373](#_Toc468805059)

[SC-12 (3) Control Enhancement 374](#_Toc468805060)

[SC-13 Cryptographic Protection 375](#_Toc468805061)

[SC-15 Collaborative Computing Devices 376](#_Toc468805062)

[SC-17 Public Key Infrastructure Certificates 378](#_Toc468805063)

[SC-18 Mobile Code 379](#_Toc468805064)

[SC-19 Voice Over Internet Protocol 380](#_Toc468805065)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) 381](#_Toc468805066)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) 382](#_Toc468805067)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service 383](#_Toc468805068)

[SC-23 Session Authenticity 384](#_Toc468805069)

[SC-28 Protection of Information at Rest 384](#_Toc468805070)

[SC-28 (1) Control Enhancement 385](#_Toc468805071)

[SC-39 Process Isolation 386](#_Toc468805072)

[13.17 System and Information Integrity (SI) 387](#_Toc468805073)

[SI-1 System and Information Integrity Policy and Procedures 387](#_Toc468805074)

[SI-2 Flaw Remediation 388](#_Toc468805075)

[SI-2 (2) Control Enhancement 390](#_Toc468805076)

[SI-2 (3) Control Enhancement 391](#_Toc468805077)

[SI-3 Malicious Code Protection 392](#_Toc468805078)

[SI-3 (1) Control Enhancement 394](#_Toc468805079)

[SI-3 (2) Control Enhancement 395](#_Toc468805080)

[SI-3 (7) Control Enhancement 396](#_Toc468805081)

[SI-4 Information System Monitoring 397](#_Toc468805082)

[SI-4 (1) Control Enhancement 400](#_Toc468805083)

[SI-4 (2) Control Enhancement 401](#_Toc468805084)

[SI-4 (4) Control Enhancement 402](#_Toc468805085)

[SI-4 (5) Control Enhancement 403](#_Toc468805086)

[SI-4 (14) Control Enhancement 403](#_Toc468805087)

[SI-4 (16) Control Enhancement 404](#_Toc468805088)

[SI-4 (23) Control Enhancement 405](#_Toc468805089)

[SI-5 Security Alerts, Advisories, and Directives 406](#_Toc468805090)

[SI-6 Security Functionality Verification 407](#_Toc468805091)

[SI-7 Software, Firmware, and Information Integrity 409](#_Toc468805092)

[SI-7 (1) Control Enhancement 410](#_Toc468805093)

[SI-7 (7) Control Enhancement 411](#_Toc468805094)

[SI-8 Spam Protection 412](#_Toc468805095)

[SI-8 (1) Control Enhancement 413](#_Toc468805096)

[SI-8 (2) Control Enhancement 414](#_Toc468805097)

[SI-10 Information Input Validation 414](#_Toc468805098)

[SI-11 Error Handling 415](#_Toc468805099)

[SI-12 Information Handling and Retention 416](#_Toc468805100)

[SI-16 Memory Protection 417](#_Toc468805101)

[14 Acronyms 419](#_Toc468805102)

[15 Attachments 422](#_Toc468805103)

[15.1 ATTACHMENT 1 - Information Security Policies and Procedures 423](#_Toc468805104)

[15.2 ATTACHMENT 2 - User Guide 425](#_Toc468805105)

[15.3 ATTACHMENT 3 – E-Authentication 426](#_Toc468805106)

[15.4 ATTACHMENT 4 – PTA / PIA 427](#_Toc468805107)

[15.5 ATTACHMENT 5 - Rules of Behavior 428](#_Toc468805108)

[15.6 ATTACHMENT 6 – Information System Contingency Plan 429](#_Toc468805109)

[15.7 ATTACHMENT 7 - Configuration Management Plan 430](#_Toc468805110)

[15.8 ATTACHMENT 8 - Incident Response Plan 431](#_Toc468805111)

[15.9 ATTACHMENT 9 - CIS Report and Worksheet 432](#_Toc468805112)

[15.10 ATTACHMENT 10 - FIPS 199 433](#_Toc468805113)

[15.11 ATTACHMENT 11 - Separation of Duties Matrix 434](#_Toc468805114)

[15.12 ATTACHMENT 12 – FedRAMP Laws and Regulations 435](#_Toc468805115)

[FedRAMP Applicable Laws 435](#_Toc468805116)

[FedRAMP Applicable Standards and Guidance 438](#_Toc468805117)

[15.13 ATTACHMENT 13 – FedRAMP Inventory Workbook 443](#_Toc468805118)

**List of Tables**

[Table 1‑1 Information System Name and Title 21](#_Toc468805119)

[Table 2‑1 Security Categorization 21](#_Toc468805120)

[Table 2‑2 Sensitivity Categorization of Information Types 23](#_Toc468805121)

[Table 2‑3 Security Impact Level 23](#_Toc468805122)

[Table 2‑4 Baseline Security Configuration 23](#_Toc468805123)

[Table 2‑5 E-Authentication Questions 24](#_Toc468805124)

[Table 2‑6 Authentication Level Determination 24](#_Toc468805125)

[Table 3‑1 Information System Owner 25](#_Toc468805126)

[Table 5‑1 Information System Management Point of Contact 25](#_Toc468805127)

[Table 5‑2 Information System Technical Point of Contact 26](#_Toc468805128)

[Table 6‑1 CSP Name Internal ISSO (or Equivalent) Point of Contact 27](#_Toc468805129)

[Table 6‑2 AO ISSO Point of Contact 27](#_Toc468805130)

[Table 7‑1 System Status 27](#_Toc468805131)

[Table 8‑1 Service Layers Represented in this SSP 28](#_Toc468805132)

[Table 8‑2 Cloud Deployment Model Represented in this SSP 29](#_Toc468805133)

[Table 8‑3 Leveraged Authorizations 29](#_Toc468805134)

[Table 9‑1 Personnel Roles and Privileges 31](#_Toc468805135)

[Table 10‑1 Ports, Protocols, and Services 34](#_Toc468805136)

[Table 11‑1 System Interconnections 35](#_Toc468805137)

[Table 12‑1 Information System Name Laws and Regulations 37](#_Toc468805138)

[Table 12‑2 Information System Name Standards and Guidance 37](#_Toc468805139)

[Table 13‑1 Summary of Required Security Controls 38](#_Toc468805140)

[Table 13‑2 Control Origination and Definitions 46](#_Toc468805141)

[Table 13‑3 CA-3 Authorized Connections 131](#_Toc468805142)

[Table 15‑1. Attachment File Naming Convention 423](#_Toc468805143)

[Table 15‑3 FedRAMP Laws and Regulations 435](#_Toc468805144)

[Table 15‑4 FedRAMP Applicable Standards and Guidance 439](#_Toc468805145)

**List of Figures**

[Figure 9‑1 Authorization Boundary Diagram 30](#_Toc468805307)

[Figure 9‑2 Network Diagram 32](#_Toc468805308)

[Figure 10‑1 Data Flow Diagram 34](#_Toc468805309)

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

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

Table ‑ Information System Name and Title

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

1. **Information System Categorization**

The overall information system sensitivity categorization is recorded in Table 2‑1 Security Categorization that follows.

Table ‑ Security Categorization

|  |  |
| --- | --- |
| System Sensitivity Level: | Choose level. |

* 1. **Information Types**

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

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

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

The potential impact is low if:

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

The potential impact is moderate if:

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

The potential impact is high if:

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

Instruction: Record your information types in the tables that follow. Record the sensitivity level for Confidentiality, Integrity, and Availability as High, Moderate, or Low. Add more rows as needed to add more information types. Use NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories, Volumes I & II, Revision 1 for guidance.

Delete this instruction from your final version of this document.

Example:

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

Table ‑ Sensitivity Categorization of Information Types

| **Information Type**  **(Use only information types from NIST SP 800-60, Volumes I and II**  **as amended)** | **NIST 800-60 identifier for Associated Information Type** | **Confidentiality** | **Integrity** | **Availability** |
| --- | --- | --- | --- | --- |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |

* 1. **Security Objectives Categorization (FIPS 199)**

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

Table ‑ Security Impact Level

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

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

Table ‑ Baseline Security Configuration

|  |  |
| --- | --- |
| **Information System Abbreviation Security Categorization** | Choose level |

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

* 1. **E-Authentication Determination**

The information system E-Authentication determination is described in Table 2‑5 E-Authentication Questions that follows. Directions for attaching the E-Authentication document may be found in the following section: ATTACHMENT 3 – E-Authentication Worksheet.

Table ‑ E-Authentication Questions

| **Select Response** | **E-Authentication Question** |
| --- | --- |
| Choose an item. | Does the system require authentication via the Internet? |
| Choose an item. | Is data being transmitted over the Internet via browsers? |
| Choose an item. | Do users connect to the system from over the Internet? |

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

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

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

The summary E-Authentication level is recorded in Table 2‑6 Authentication Level Determination that follows.

Table ‑ Authentication Level Determination

| **E-Authentication Determination** | |
| --- | --- |
| **System Name** | Information System Name |
| **System Owner** | <Enter System Owner>. |
| **Assurance Level** | Choose level. |
| **Date Approved** | <Select Date> |

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

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

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

1. **Information System Owner**

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

Table ‑ Information System Owner

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

1. **Authorizing Official**

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

JAB P-ATO: Federal Risk Authorization Management Program (FedRAMP) Joint Authorization Board (JAB,) as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS)

Agency 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.

1. **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 ‑ 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 ‑ 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> |

1. **Assignment of Security Responsibility**

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

Table ‑ 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 ‑ AO ISSO Point of Contact

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

1. **Information System Operational Status**

The system is currently in the life-cycle phase shown in Table 7‑1 System Status that follows.

Table ‑ 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. |

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator. (Only operational systems can be granted an ATO).

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

1. **Information System Type**

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

## Cloud Service Models

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

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

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

Instruction: Check all layers that apply.

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

Table ‑ 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: |

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

## Cloud Deployment Models

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

Instruction: Check deployment model that applies.

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

Table ‑ 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) |

## Leveraged Authorizations

Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. See the section on Use Cases in Guide to Understanding FedRAMP for more information. If a lower level layer has been granted an Authorization, and another higher level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows.

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

The Information System Abbreviation plans to leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Information System Abbreviation are listed in Table 8‑3 Leveraged Authorizations that follows.

Table ‑ Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
| <Enter Leveraged information system name> | <Enter service provider> | <Date> |
| <Enter Leveraged information system name> | <Enter service provider> | <Date> |

# General System Description

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

## System Function or Purpose

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

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

## Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system’s Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system.

Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

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

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

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

|  |
| --- |
|  |

Figure ‑ Authorization Boundary Diagram

## Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9‑1 Personnel Roles and Privileges that follows.

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

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

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

Table ‑ Personnel Roles and Privileges

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

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

## Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, DNS servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams. Assessors should be able to easily map hardware, software, and network inventories back to this diagram.

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

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 Information System Abbreviation.

|  |
| --- |
|  |

Figure ‑ Network Diagram

# System Environment

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

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

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

## Hardware Inventory

Use the FedRAMP Inventory Workbook to list the principal hardware components for Information System Abbreviation.

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

## Software Inventory

Use the FedRAMP Inventory Workbook to list the principal software components for Information System Abbreviation.

## Network Inventory

Use the FedRAMP Inventory Workbook to list the principal network devices and components for Information System Abbreviation.

## Data Flow

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

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

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

|  |
| --- |
|  |

Figure ‑ Data Flow Diagram

## 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 ‑ 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> |

# System Interconnections

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Indicate how the connection is being secured. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13‑3 CA-3 Authorized Connections.

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

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

Table ‑ System Interconnections

| SP IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) | Data Direction  (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/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> |

# Laws, Regulations, Standards, and Guidance

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

## Applicable Laws and Regulations

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

Table ‑ Information System Name Laws and Regulations

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference ID> | <Ref Date>. | <Reference ID> |
| <Reference ID> | <Reference ID> | <Ref Date>. | <Reference ID> |
| <Reference ID> | <Reference ID> | <Ref Date>. | <Reference ID> |

## APPLICABLE STANDARDS AND GUIDANCE

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

Table ‑ Information System Name Standards and Guidance

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference ID> | <Ref Date>. | <Reference ID> |
| <Reference ID> | <Reference ID> | <Ref Date>. | <Reference ID> |
| <Reference ID> | <Reference ID> | <Ref Date>. | <Reference ID> |

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

Systems that are categorized as FIPS 199 Low use the controls designated as Low, 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 ‑ 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 |
| 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 | 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) |
| 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) |
| 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 |
| 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 |
| 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 | Not Selected | SI-16 | SI-16 |

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

Instruction: In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

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

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

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

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

Table ‑ 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 CSP Name 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. |

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

## Access Control (AC)

### AC-1 Access Control Policy and Procedures Requirements

The organization:

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

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-1(a): [TBD by Customer] | |
| Parameter AC-1(b)(1): [TBD by Customer] | |
| Parameter AC-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  *[AWS customers are responsible for developing policies and procedures that apply specifically to the application]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b1 | Application  *[AWS customers are responsible for developing policies and procedures that apply specifically to the application]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b2 | Application  *[AWS customers are responsible for developing policies and procedures that apply specifically to the application]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-2 Account Management

The organization:

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

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-2(a): [TBD by Customer] | |
| Parameter AC-2(e): [TBD by Customer] | |
| Parameter AC-2(f): [TBD by Customer] | |
| Parameter AC-2(j): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization (Refer to Table 8-3) | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the AWS administrators. Through the AWS Management console and API Endpoints AWS will provide the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part h | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part i | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part j | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part k | Application  [*AWS customers are responsible for account management within their AWS application. AWS customers are responsible for properly using IAM in order to create user accounts within their AWS account, as well as properly enforcing accounts within their EC2 instances, as well as any applications they install on EC2.*  *AWS customers should review the IAM best practices website and implement them within their account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html]  Infrastructure  [AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

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

| AC-2 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly implementing the use of IAM within their account, as well as for federating identity with their on-premise LDAP/AD if required by their access control policy: https://aws.amazon.com/iam/details/manage-federation/]*  Infrastructure  *[AWS is responsible for account management of the internal users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS will provide the means for a customer to manage their top-level AWS account and IAM users. ]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-2(2)1: [TBD by Customer] | |
| Parameter AC-2(2)2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly managing any temporary or emergency accounts within their AWS application.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-2(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (3) What is the solution and how is it implemented |
| --- |
| Application  *[AWS customers can enforce lockout due to inactivity for their IAM accounts by requiring users to change their password after a period determined by their access control policy, or through the use of federation to enforce the policy using their existing directory services (LDAP) policies.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-2(4): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (4) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for auditing the creation of new IAM accounts.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints, AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-2(5): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (5) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for enforcing their organization’s inactivity policy within their AWS workloads.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [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: [TBD by Customer] | |
| Parameter AC-2(7)(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for managing their privileged accounts in accordance with their internal policies, to include host root accounts and all privileged IAM users for their account.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for managing their privileged accounts in accordance with their internal policies, to include host root accounts and all privileged IAM users for their account.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for managing their privileged accounts in accordance with their internal policies, to include host root accounts and all privileged IAM users for their account.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-2(9): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing and managing all group and/or shared accounts in accordance with their organizations access control policy.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing their AWS application’s accounts in accordance with their organizations access control policy.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### AC-2 (11) Control Enhancement

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

| AC-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-2 (11)-1: [TBD by Customer] | |
| Parameter AC-2 (11)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (11) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing their AWS application’s and IAM accounts in accordance with their organizations access control policy.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

1. Monitors information system accounts for [Assignment: organization-defined atypical use]; and
2. 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) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-2(12)(a): [TBD by Customer] | |
| Parameter AC-2(12)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for implementing auditing capability that provides monitoring to detect atypical usage of their account.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for implementing auditing capability that provides monitoring to detect atypical usage of their account.]*  Infrastructure  *[AWS is responsible for account management of the internal AWS users of the AWS infrastructure. Through the AWS Management console and API Endpoints AWS provides the means for a customer to manage their top-level AWS account and IAM users.]*  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-3 Access Enforcement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for establishing a process for approving logical access to their AWS application’s and the IAM management console, ensuring that the process is performed in accordance with the customer’s access control policy and the authorizations granted to the system users are approved as required.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-4 Information Flow Enforcement

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: [TBD by Customer] | |
| Parameter AC-4: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-4 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for establishing and enforcing information flow control for their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-4(21)-1: [TBD by Customer] | |
| Parameter AC-4(21)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for establishing and enforcing information flow control for their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-5 Separation of Duties

The organization:

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

AC-5 Additional FedRAMP Requirements and Guidance:

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

| AC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-5(a): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for properly configuring their AWS application’s and IAM accounts permissions as it relates to the application and guest operating system in order to enforce separation of duties within their AWS account and application.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for documenting the separation of duties as it relates to the application, guest operating systems and IAM accounts.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for properly defining the access authorizations to support the separation of duties as it relates to the application, guest operating systems and IAM accounts.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-6 Least Privilege

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

| AC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-6 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly configuring IAM accounts and user permissions within their application and guest operating system in order to enforce least privilege].*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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 |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-6(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly configuring their AWS IAM accounts and their application and guest operating system to restrict access to all security-relevant functions and information].*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-6(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for creating non-privileged accounts as it relates to their application and guest operating system for accessing non-security functions.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### AC 6 (5) Control Enhancement

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

| AC-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-6 (5): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for authorizing and documenting the users or roles as it relates to their application, guest operating system and with privileged access to their AWS account.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly auditing the execution of privileged functions within their account as it relates to their IAM accounts, application and guest operating system.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for configuring IAM, application and guest operating system accounts to restrict non-privileged users from altering security safeguards.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-7 Unsuccessful Login Attempts

The organization:

1. Enforces a limit of [FedRAMP Assignment: not more than three (3)] consecutive invalid logon attempts by a user during a [FedRAMP Assignment: fifteen (15) minutes]; and
2. Automatically [Selection: locks the account/node for 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: [TBD by Customer] | |
| Parameter AC-7(a)-1: [TBD by Customer] | |
| Parameter AC-7(a)-2: [TBD by Customer] | |
| Parameter AC-7(b)-1: [TBD by Customer] | |
| Parameter AC-7(b)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for implementing account lockout. They need to consider both IAM accounts as well as accounts associated with their workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for implementing account lockout. They need to consider both IAM accounts as well as accounts associated with their workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-8 System Use Notification

The information system:

1. 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;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [Assignment: organization-defined conditions (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: [TBD by Customer] | |
| Parameter AC-8(a): [TBD by Customer] | |
| Parameter AC-8(c)-1: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for displaying a system use notification or banner before granting access within their hosted systems/applications.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for ensuring a system use notification or banner is acknowledged before granting access within their hosted systems/applications.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for displaying a system use notification or banner before granting access within their hosted systems/applications that are publicly accessible.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Application  *[AWS customers are responsible for determining which elements of their hosted systems/applications require a system use notification or banner.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Req. 2 | Application  *[AWS customers are responsible for determining how a system use notification or banner within their hosted systems/applications will be verified.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Req. 3 | Application  *[AWS customers are responsible for having a documented agreement to provide results of verification among the system use notification or banner.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-10 Concurrent Session Control

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: [TBD by Customer] | |
| Parameter AC-10-1: [TBD by Customer] | |
| Parameter AC-10-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-10 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for limiting concurrent sessions to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-11 Session Lock

The information system:

1. 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
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-11(a): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for enabling session lock on their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for configuring appropriate session lock controls for their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers must ensure session lock mechanisms, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-12 Session Termination

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: [TBD by Customer] | |
| Parameter AC-12: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-12 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for configuring access to their IAM account and AWS application to terminate due to a defined period of inactivity.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-14 Permitted Actions without Identification or Authentication

The organization:

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

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-14(a): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for identifying, authorizing and documenting the actions that are allowed without identity and authentication within their AWS account and workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for identifying, authorizing and documenting the actions that are allowed without identity and authentication within their AWS account and workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-17 Remote Access

The organization:

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

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for documenting and implementing remote access methods to their workloads deployed on AWS infrastructure*.*]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for authorizing remote access to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for monitoring remote access to their AWS account and their workloads deployed on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| AC-17 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for using encryption when remotely accessing their AWS account and application, to include ensuring they are making use of API endpoints that support appropriate encrypted connections. Customers must also install and manage cryptographic modules on their workloads to manage their client connections.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-17(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for configuring their VPC’s Internet gateways to properly restrict remote access to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| AC-17 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-17(4)(a): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[All customer access to AWS is done via remote connections. AWS customers are responsible for documenting and implementing remote access to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[All customer access to AWS is done via remote connections. AWS customers are responsible for documenting and implementing remote access to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-17(9): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for providing a mechanism to terminating remote access to their workloads deploy on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-18 Wireless Access

The organization:

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

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for properly configuring all wireless devices that connect to their workloads deployed on AWS infrastructure].*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for properly configuring all wireless devices that connect to their workloads deployed on AWS infrastructure].*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-18 (1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly configuring all wireless devices that connect to their workloads deployed on AWS infrastructure].*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-19 Access Control for Mobile Devices

The organization:

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

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for authorizing the use of portable/mobile devices if they are used to connect to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for authorizing the use of portable/mobile devices if they are used to connect to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-19(5)-1: [TBD by Customer] | |
| Parameter AC-19(5)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-19 (5) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for deploying encryption on mobile devices used to access their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-20 Use of External Information Systems

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

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

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for establishing terms and conditions with third-party organizations connecting to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for establishing terms and conditions with third-party organizations connecting to their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

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

| AC-20 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for establishing the verification and approval agreements of any external information systems permitted to access their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for establishing the verification and approval agreements of any external information systems permitted to access their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AC-20(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for developing policies regarding the use of portable storage devices.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-21 Information Sharing

The organization:

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

| AC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-21(a): [TBD by Customer] | |
| Parameter AC-21(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for properly protecting their sensitive data stored as part of their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for properly protecting their sensitive data stored as part of their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AC-22 Publicly Accessible Content

The organization:

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

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AC-22: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for properly controlling public information posted on websites or in their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for properly controlling public information posted on websites or in their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for properly controlling public information posted on websites or in their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  *[AWS customers are responsible for properly controlling public information posted on websites or in their workloads deployed on AWS infrastructure.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter AT-1(a): [TBD by Customer] | |
| Parameter AT-1(b)(1): [TBD by Customer] | |
| Parameter AT-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AT-2 Security Awareness

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

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

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AT-2(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| AT-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AT-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AT-3 Role-Based Security Training

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

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

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AT-3(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AT-4 Security Training Records

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [FedRAMP Assignment: at least five (5) years or 5 years after completion of a specific training program].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AT-4(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing security awareness and training for their employees.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter AU-1(a): [TBD by Customer] | |
| Parameter AU-1(b)(1): [TBD by Customer] | |
| Parameter AU-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-2 Audit Events

The organization:

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

AU-2 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: [TBD by Customer] | |
| Parameter AU-2(a): [TBD by Customer] | |
| Parameter AU-2(d): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for establishing, implementing, reviewing configuring and updating auditable events on their storage resources and virtual machines, based on a risk assessment and mission/business needs. The collection and protection of these audits belongs to the customer as well.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for establishing, implementing, reviewing configuring and updating auditable events on their storage resources and virtual machines, based on a risk assessment and mission/business needs. The collection and protection of these audits belongs to the customer as well.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for establishing, implementing, reviewing configuring and updating auditable events on their storage resources and virtual machines, based on a risk assessment and mission/business needs. The collection and protection of these audits belongs to the customer as well.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for establishing, implementing, reviewing configuring and updating auditable events on their storage resources and virtual machines, based on a risk assessment and mission/business needs. The collection and protection of these audits belongs to the customer as well.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AU-2(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for reviewing their auditable events policy on an annual basis.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-3 Content of Audit Records

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing auditing on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AU-3(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing auditing on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-4 Audit Storage Capacity

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

| AU-4 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AU-4: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for ensuring that sufficient storage is allocated for their audit logs. This can be accomplished using S3 to properly archive their audit logs. S3 satisfies the requirement to expand audit log storage capability on demand for customers.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-5 Response to Audit Processing Failures

The information system:

1. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
2. Takes the following additional actions: [FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AU-5(a): [TBD by Customer] | |
| Parameter AU-5(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for configuring alarms or notifications in order to notify administrators of audit log failures within their AWS workloads. Customer administrators are responsible for responding to audit failures.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for configuring alarms or notifications in order to notify administrators of audit log failures within their AWS workloads. Customer administrators are responsible for responding to audit failures.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-6 Audit Review, Analysis, and Reporting

The organization:

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

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines audit record types [FedRAMP Assignment: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.].

| AU-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AU-6(a)-1: [TBD by Customer] | |
| Parameter AU-6(a)-2: [TBD by Customer] | |
| Parameter AU-6(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for reviewing audit logs generated on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for reviewing audit logs generated on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for establishing automated mechanisms for reviewing audit logs generated on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| AU-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for reviewing audit logs generated on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-7 Audit Reduction and Report Generation

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

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

| AU-7 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for reviewing audit logs generated by their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for reviewing audit logs generated by their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AU-7(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-7 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for reviewing audit logs generated by their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-8 Time Stamps

The information system:

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

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AU-8(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The information system:

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

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

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

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

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

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server

| AU-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AU-8(1)(a)-1: [TBD by Customer] | |
| Parameter AU-8(1)(a)-2: [TBD by Customer] | |
| Parameter AU-8(1)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

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

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

| AU-8 (1) Req. | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Application  *[AWS customers are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Req. 2 | Application  *[AWS customers are responsible for configuring their EC2 instances to synchronize with the ntp servers required by their organization.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-9 Protection of Audit Information

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

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly protecting audit data generated by their AWS workloads. Customers can protect their audit data through the proper implementation of encryption of data at rest, as well as through implementation of access policies to restrict access to audit data to authorized users.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AU-9(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly backing up audit logs from on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter AU-9(4): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for protecting their audit data through the proper implementation of encryption at rest, as well as through implementation of access policies to restrict access to audit data to authorized users.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-11 Audit Record Retention

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: [TBD by Customer] | |
| Parameter AU-11: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for storing their audit logs to preserve them for the period required by their organization. This can be accomplished using S3.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### AU-12 Audit Generation

The information system:

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

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter AU-12(a): [TBD by Customer] | |
| Parameter AU-12(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for audit logs generated on their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for audit logs generated on their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for audit logs generated on their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Security Assessment and Authorization (CA)

### CA-1 Security Assessment and Authorization Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter CA-1(a): [TBD by Customer] | |
| Parameter CA-1(b)(1): [TBD by Customer] | |
| Parameter CA-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-2 Security Assessments

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [FedRAMP Assignment: at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [FedRAMP Assignment: individuals or roles to include the FedRAMP PMO].

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-2(b): [TBD by Customer] | |
| Parameter CA-2(d): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-2 (1) Control Enhancement

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 3PAO.

| CA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-2(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-2 (2) Control Enhancement

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: [TBD by Customer] | |
| Parameter CA-2(2)-1: [TBD by Customer] | |
| Parameter CA-2(2)-2: [TBD by Customer] | |
| Parameter CA-2(2)-3: [TBD by Customer] | |
| Parameter CA-2(2)-4: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-2 (3) Control Enhancement

The organization accepts the results of an assessment of [FedRAMP Assignment: any FedRAMP Accredited 3PAO] 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: [TBD by Customer] | |
| Parameter CA-2(3)-1: [TBD by Customer] | |
| Parameter CA-2(3)-2: [TBD by Customer] | |
| Parameter CA-2(3)-3: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing their organization’s risk assessment policy and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-3 System Interconnections

The organization:

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

Table ‑ 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 |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-3(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing any necessary Interconnection Security Agreements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing any necessary Interconnection Security Agreements.  See Table 13‑2 Control Origination and Definitions and Table 11‑1 System Interconnections for information about implementation.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing any necessary Interconnection Security Agreements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-3 (3) Control Enhancement

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

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

| CA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-3(3)-1: [TBD by Customer] | |
| Parameter CA-3(3)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly designing and deploying boundary protections for connections to their applications hosted on AWS, to include satisfying TIC requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-3 (5) Control Enhancement

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: [TBD by Customer] | |
| Parameter CA-3(5)-1: [TBD by Customer] | |
| Parameter CA-3(5)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for architecting and implementing information flow policies to meet their system requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-5 Plan of Action and Milestones

The organization:

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

CA-5 Additional FedRAMP Requirements and Guidance:

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

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-5(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing and maintaining a POA&M for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing and maintaining a POA&M for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-6 Security Authorization

The organization:

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

CA-6c Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-6(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for working with a federal agency to assign an authorizing official for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for attaining authorization for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for attaining authorization for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-7 Continuous Monitoring

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

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

| CA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-7(a): [TBD by Customer] | |
| Parameter CA-7(b)-1: [TBD by Customer] | |
| Parameter CA-7(b)-2: [TBD by Customer] | |
| Parameter CA-7(g)-1: [TBD by Customer] | |
| Parameter CA-7(g)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Req. 2 | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Req. 3 | Application  [AWS customers are responsible for developing a continuous monitoring strategy for their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-7 (1) Control Enhancement

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: [TBD by Customer] | |
| Parameter CA-7(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for selecting an independent assessor to validate the continuous monitoring of their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-8 Penetration Testing

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

| CA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-8-1: [TBD by Customer] | |
| Parameter CA-8-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-8 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for penetration testing of their systems running on AWS including coordination with AWS when penetration testing is scheduled.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### CA-8 (1) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-8 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for penetration testing of their systems running on AWS, including notifying AWS when penetration testing is scheduled.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CA-9 Internal System Connections

The organization:

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

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CA-9(a): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for documenting and authorizing the configuration of security groups and network ACLs within their VPCs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for documenting and authorizing the configuration of security groups and network ACLs within their VPCs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures

The organization:

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

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-1(a): [TBD by Customer] | |
| Parameter CM-1(b)(1): [TBD by Customer] | |
| Parameter CM-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-2 Baseline Configuration

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

| CM-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

1. [FedRAMP Assignment: at least annually or when a significant change occurs];
2. When required due to [FedRAMP Assignment: to include when directed by the JAB]; and
3. 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: [TBD by Customer] | |
| Parameter CM-2(1)(a): [TBD by Customer] | |
| Parameter CM-2(1)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization retains [FedRAMP Assignment: organization-defined previous versions of baseline configurations of the previously approved baseline configuration of IS components] to support rollback.

| CM-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-2(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining previous versions of the baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| CM-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance Manager | |
| Parameter CM-2(7)(a)-1: Amazon managed assets | |
| Parameter CM-2(7)(a)-2: full-disk encryption | |
| Parameter CM-2(7)(b): securely wiped | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for creating a policy for issuing devices that are part of the information system to personnel when travelling to locations that it has deemed a significant risk.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for creating a policy for issuing devices that are part of the information system to personnel when travelling to locations that it has deemed a significant risk.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-3 Configuration Change Control

The organization:

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

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

Guidance: In accordance with record retention policies and procedures.

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

CM-3 Additional FedRAMP Requirements and Guidance:

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

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-3(e): [TBD by Customer] | |
| Parameter CM-3(g)-1: [TBD by Customer] | |
| Parameter CM-3(g)-2: [TBD by Customer] | |
| Parameter CM-3(g)-3: [TBD by Customer] | |
| Parameter CM-3(g)-4: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration of their systems deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-4 Security Impact Analysis

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

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

| CM-4 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing configuration management, to include conducting security impact analyses of proposed changes to their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-5 Access Restrictions for Change

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-5 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for defining, approving and enforcing physical and logical access restrictions to their AWS accounts and systems.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| CM-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for restricting access and auditing of their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter CM-5(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing digital signatures within applications hosted on EC2 to ensure that installed software has been signed using an approved certificate.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| CM-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-5(5)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for restricting access to their AWS account, and periodically reviewing and reevaluating system change privileges.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for restricting access to their AWS account, and periodically reviewing and reevaluating system change privileges.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-6 Configuration Settings

The organization:

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

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

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

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

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

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

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-6(a)-1: [TBD by Customer] | |
| Parameter CM-6(a)-2: [TBD by Customer] | |
| Parameter CM-6(c)-1: [TBD by Customer] | |
| Parameter CM-6(c)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter CM-6(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-7 Least Functionality

The organization:

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

CM-7 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. 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://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-7(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| CM-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-7(1)(a): [TBD by Customer] | |
| Parameter CM-7(1)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: AWS Security Assurance Manager | |
| Parameter CM-7(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for restricting what software is allowed to run in their AWS account and their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization].. |

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

The organization:

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

| CM-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-7(5)(a): [TBD by Customer] | |
| Parameter CM-7(5)(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for configuration settings within their AWS account and any software they install on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-8 Information System Component Inventory

The organization:

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

CM-8 Additional FedRAMP Requirements and Guidance:

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

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-8(a)(4): [TBD by Customer] | |
| Parameter CM-8(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and complete inventory of their systems deployed on AWS. AWS customers can choose to use AWS Config (Optional) in order to maintain an inventory of their AWS resources:  <https://aws.amazon.com/config/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and complete inventory of their systems deployed on AWS. AWS customers can choose to use AWS Config (Optional) in order to maintain an inventory of their AWS resources:  <https://aws.amazon.com/config/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-8 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and complete inventory of their systems deployed on AWS. AWS customers can choose to use AWS Config (Optional) in order to maintain an inventory of their AWS resources:  <https://aws.amazon.com/config/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| CM-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-8(3)(a): [TBD by Customer] | |
| Parameter CM-8(3)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and complete inventory of their systems deployed on AWS. AWS customers can choose to use AWS Config (Optional) in order to maintain an inventory of their AWS resources:  <https://aws.amazon.com/config/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and complete inventory of their systems deployed on AWS. AWS customers can choose to use AWS Config (Optional) in order to maintain an inventory of their AWS resources:  <https://aws.amazon.com/config/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing configuration management, to include maintaining a baseline configuration and a complete inventory of their systems deployed on AWS. AWS customers can choose to use AWS Config (Optional) in order to maintain an inventory of their AWS resources:  <https://aws.amazon.com/config/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-9 Configuration Management Plan

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

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

| CM-9 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management, to include developing a configuration management plan.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management, to include developing a configuration management plan.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing configuration management, to include developing a configuration management plan.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for properly implementing configuration management, to include developing a configuration management plan.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-10 Software Usage Restrictions

The organization:

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

| CM-10 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management to include any software usage restrictions.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management to include any software usage restrictions.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing configuration management to include any software usage restrictions.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter CM-10(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-10 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for documenting and implementing restrictions on the use of open source software.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CM-11 User-Installed Software

The organization:

1. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
2. Enforces software installation policies through [Assignment: organization-defined methods]; and
3. Monitors policy compliance [FedRAMP Assignment: Continuously (via CM-7 (5))].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CM-11(a): [TBD by Customer] | |
| Parameter CM-11(b): [TBD by Customer] | |
| Parameter CM-11(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing configuration management.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing configuration management.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing configuration management.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures

The organization:

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

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CP-1(a): [TBD by Customer] | |
| Parameter CP-1(b)(1): [TBD by Customer] | |
| Parameter CP-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-2 Contingency Plan

The organization:

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

CP-2 Additional FedRAMP Requirements and Guidance:

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

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CP-2(a)(6): [TBD by Customer] | |
| Parameter CP-2(b): [TBD by Customer] | |
| Parameter CP-2(d): [TBD by Customer] | |
| Parameter CP-2(f): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| CP-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-2 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter CP-2(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| CP-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-3 Contingency Training

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

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

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CP-3(a): [TBD by Customer] | |
| Parameter CP-3(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-3 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-4 Contingency Plan Testing

The organization:

1. 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.

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

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CP-4(a)-1: [TBD by Customer] | |
| Parameter CP-4(a)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| CP-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-6 Alternate Storage Site

The organization:

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

| CP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-7 Alternate Processing Site

The organization:

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

CP-7a Additional FedRAMP Requirements and Guidance:

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

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

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CP-7(a)-1: [TBD by Customer] | |
| Parameter CP-7(a)-2: CP-7 Additional FedRAMP Requirements and Guidance | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-8 Telecommunications Services

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: [TBD by Customer] | |
| Parameter CP-8-1: immediate resumption using a redundant communications path | |
| Parameter CP-8-2: the service provider defines a time period consistent with the business impact analysis | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-8 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| CP-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-9 Information System Backup

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

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

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

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

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

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

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

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

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

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

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter CP-9(a): [TBD by Customer] | |
| Parameter CP-9(b): [TBD by Customer] | |
| Parameter CP-9(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS customers are responsible for properly backing up their data, to include taking regular EBS snapshots to ensure that EBS volume backups are replicated across the entire region.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS customers are responsible for properly backing up their data, to include taking regular EBS snapshots to ensure that EBS volume backups are replicated across the entire region.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS customers are responsible for properly backing up their data, to include taking regular EBS snapshots to ensure that EBS volume backups are replicated across the entire region.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS customers are responsible for properly backing up their data, to include taking regular EBS snapshots to ensure that EBS volume backups are replicated across the entire region.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter CP-9 (1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter CP-9(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### CP-10 Information System Recovery and Reconstitution

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| CP-10 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Reviews and updates the current:
   1. Identification and authentication policy [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: [TBD by Customer] | |
| Parameter IA-1(a): [TBD by Customer] | |
| Parameter IA-1(a): [TBD by Customer] | |
| Parameter IA-1(b)(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IA-2 Identification and Authentication (Organizational Users)

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

| IA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 What is the solution and how is it implemented? |
| --- |
| Application  [The master account and IAM accounts are used by customers to manage identification and authentication of the customers AWS services. They can be configured with varying levels of permissions, and are used to set up and design the system: http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### IA-2 (1) Control Enhancement

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

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| Application  [*AWS customers are responsible for establishing MFA for use with their AWS account:*  <https://aws.amazon.com/iam/details/mfa/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  [*AWS customers are responsible for establishing Multifactor Authentication (MFA) for use with their AWS account:*  <https://aws.amazon.com/iam/details/mfa/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Information Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (3) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (5) What is the solution and how is it implemented? |
| --- |
| Application  *Recommend AWS customers use permission groups and IAM users rather than sharing credentials within their IAM account:*  http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IA-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (8) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing replay-resistant authentication mechanisms for network access to privileged accounts.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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].

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: [TBD by Customer] | |
| Parameter IA-2(11): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (11) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing MFA using devices that are separate from the system gaining access and are validated via FIPS, NIAP, or NSA validation programs].*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### IA-2 (12) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS provides federation capabilities, which can be used by customers to establish PIV authentication for IAM users within their account. Implementing PIV authentication for any application deployed on an AWS workload is the responsibility of the customer.]*  Infrastructure  Reference the pre-existing FedRAMP Provisional Authorization to Operate (P-ATO) for AWS GovCloud (US), 6/21/2016 |

### IA-3 Device Identification and Authentication

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: [TBD by Customer] | |
| Parameter IA-3-1: [TBD by Customer] | |
| Parameter IA-3-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-3 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for properly configuring any devices that will remotely connect to their AWS resources.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IA-4 Identifier Management

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

1. 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;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years]; and
5. 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: [TBD by Customer] | |
| Parameter IA-4(a): [TBD by Customer] | |
| Parameter IA-4(d): [TBD by Customer] | |
| Parameter IA-4(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>. The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>. The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>. The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>. The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>. The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IA-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IA-4 (4): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-4 (4) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing identifiers within their IAM account as well as those associated with their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IA-5 Authenticator Management

The organization manages information system authenticators by:

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

IA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Authenticators must be compliant with NIST SP 800-63-2 Electronic Authentication Guideline assurance Level 4. Link to publication: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IA-5(g): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html. The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part h | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part i | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part j | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The information system, for password-based authentication:

1. Enforces minimum password complexity of [FedRAMP Assignment: case sensitive, minimum of fourteen (14) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters];
2. Enforces at least the following number of changed characters when new passwords are created: [FedRAMP Assignment: at least fifty percent (50%)];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [FedRAMP Assignment: one (1) day minimum, sixty (60) day maximum];
5. Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IA-5(1)(a): [TBD by Customer] | |
| Parameter IA-5(1)(b): [TBD by Customer] | |
| Parameter IA-5(1)(d): [TBD by Customer] | |
| Parameter IA-5(1)(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [The master account and IAM accounts are used by customers to manage identification and authorization. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The information system, for PKI-based authentication:

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

| IA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing and managing PKI that is part of their system running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing and managing PKI that is part of their system running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing and managing PKI that is part of their system running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for implementing and managing PKI that is part of their system running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

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

| IA-5 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly distributing their MFA authenticators.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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 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: [TBD by Customer] | |
| Parameter IA-5(4): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 (4) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring the password implementation on their AWS workloads, as well as within IAM.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 (6) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring the password implementation on their AWS workloads, as well as within IAM.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 (7) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring the password implementation on their AWS workloads, as well as within IAM.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### IA-5 (11) Control Enhancement

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: [TBD by Customer] | |
| Parameter IA-5(11): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for either using MFA provided by AWS, or implementing one that satisfies their requirements, and using that solution through federation.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IA-6 Authenticator Feedback

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-6 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for obfuscating passwords that are used in conjunction with system being run on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IA-7 Cryptographic Module Authentication

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-7 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing authentication to cryptographic modules in accordance with applicable laws and regulations.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-8 What is the solution and how is it implemented? |
| --- |
| Application  [The master account and IAM accounts are used by customers to manage identification and authorization of their AWS account. They can be configured with varying levels of permissions, and are used to set up and design the system: <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The accounts that customers create on their guest operating systems and VMs are completely separate and are the responsibility of the customer to manage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### IA-8 (1) Control Enhancement

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

| IA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
| *[AWS provides federation capabilities, which can be used by customers to establish PIV authentication for IAM users within their account. Implementing PIV authentication for any application deployed on an AWS workload is the responsibility of the customer.]* |

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

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

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
| *[AWS provides identity federation capabilities that can be used to implement FICAM-approved credentials for IAM users within an AWS account. Implementation of FICAM-approved credentials is the responsibility of the customer.]* |

#### IA-8 (3) Control Enhancement

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: [TBD by Customer] | |
| Parameter IA-8(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
| *[AWS provides identity federation capabilities that can be used to implement FICAM-approved credentials for IAM users within an AWS account. Implementation of FICAM-approved credentials is the responsibility of the customer.]* |

#### IA-8 (4) Control Enhancement

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
| *[AWS provides identity federation capabilities that can be used to implement FICAM-approved credentials for IAM users within an AWS account. Implementation of FICAM-approved credentials is the responsibility of the customer.]* |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures

The organization:

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

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-1(a): [TBD by Customer] | |
| Parameter IR-1(b)(1): [TBD by Customer] | |
| Parameter IR-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-2 Incident Response Training

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

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

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-2(a): [TBD by Customer] | |
| Parameter IR-2(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for providing incident response training when new personnel assume an incident response role, as required by system changes and annually thereafter.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for providing incident response training when new personnel assume an incident response role, as required by system changes and annually thereafter.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for providing incident response training when new personnel assume an incident response role, as required by system changes and annually thereafter.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-3 Incident Response Testing

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: [TBD by Customer] | |
| Parameter IR-3-1: [TBD by Customer] | |
| Parameter IR-3-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-3 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IR-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-3 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-4 Incident Handling

The organization:

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

IR-4 Additional FedRAMP Requirements and Guidance:

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

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

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing an incident handling capability that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing an incident handling capability that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing an incident handling capability that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IR-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for employing automated mechanisms to support the incident handling process.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-5 Incident Monitoring

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-5 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for tracking and documenting their information system security incidents.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-6 Incident Reporting

The organization:

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

IR-6 Additional FedRAMP Requirements and Guidance

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

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-6(a): [TBD by Customer] | |
| Parameter IR-6(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IR-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-6 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-7 Incident Response Assistance

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-7 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for providing 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.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IR-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-7 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for providing 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.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

The organization:

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

| IR-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-7 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for establishing external cooperative relationships with providers of information system protection capabilities and identifying internal incident response team members as applicable.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for establishing external cooperative relationships with providers of information system protection capabilities and identifying internal incident response team members as applicable.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-8 Incident Response Plan

The organization:

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

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

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

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

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

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

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

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-8(a)(8): [TBD by Customer] | |
| Parameter IR-8(b): [TBD by Customer] | |
| Parameter IR-8(c): [TBD by Customer] | |
| Parameter IR-8(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for developing IR plans and testing that includes consideration for any controls deferred to the customer relating to shared touch points included in the AWS authorization boundary and any customer applications leveraging the AWS infrastructure.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### IR-9 Information Spillage Response

The organization responds to information spills by:

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

| IR-9 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-9(b): [TBD by Customer] | |
| Parameter IR-9(f): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for identifying the information involved in an information system contamination, as AWS does not manage customer data or determine its categorization. AWS has no insight into the sensitivity of customer data, and must consequently treat all customer data as sensitive. As such, only a customer can determine whether data has been spilled on an EC2 instance, an EBS volume or S3 object.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for identifying the information involved in an information system contamination, as AWS does not manage customer data or determine its categorization. AWS has no insight into the sensitivity of customer data, and must consequently treat all customer data as sensitive. As such, only a customer can determine whether data has been spilled on an EC2 instance, an EBS volume or S3 object.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly isolating any EC2 instance or EBS volume that is currently hosting spilled data. Similarly, the customer is responsible for removing logical access to any S3 object that contains spillage.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [*AWS customers can perform traditional overwrite practices on EC2 instances and EBS volumes in order to sanitize the environment, and subsequently terminate the EC2 instance or delete of the EBS volume. To destroy an S3 object, the customer will delete the encryption key that controls access to it, and delete the S3 object, breaking the mapping to it. ]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for determining which of their AWS assets contains spillage, or if the spillage extends to their on-premise assets.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for conducting forensic and remediation activities in accordance with their organization’s spillage policies.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IR-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-9(1): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-9 (1) What is the solution and how is it implemented? |
| --- |
| Application  [*AWS customers are responsible for identifying the information involved in an information system contamination, as AWS does not manage customer data or determine its categorization. AWS has no insight into the sensitivity of customer data, and must consequently treat all customer data as sensitive. As such, only a customer can determine whether data has been spilled on an EC2 instance, an EBS volume or S3 object.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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

| IR-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter IR-9(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-9 (2) What is the solution and how is it implemented? |
| --- |
| Application  [*AWS customers are responsible for providing information spillage response training.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter IR-9(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-9 (3) What is the solution and how is it implemented? |
| --- |
| *[AWS customers are responsible for developing procedures that allow operations to be maintained while responding to a data spill within their AWS environment. The AWS environment allows customers to easily deploy a known good version of their environment while preserving contaminated instances for forensic investigation.*  *AWS customers are responsible for identifying the information involved in an information system contamination, as AWS does not manage customer data or determine its categorization. AWS has no insight into the sensitivity of customer data, and must consequently treat all customer data as sensitive. As such, only a customer can determine whether data has been spilled on an EC2 instance, an EBS volume or S3 object.]* |

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

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: [TBD by Customer] | |
| Parameter IR-9(4): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| IR-9 (4) What is the solution and how is it implemented? |
| --- |
| *[AWS customers are responsible for developing procedures that allow operations to be maintained while responding to a data spill within their AWS environment. The AWS environment allows customers to easily deploy a known good version of their environment while preserving contaminated instances for forensic investigation.*  *AWS customers are responsible for identifying the information involved in an information system contamination, as AWS does not manage customer data or determine its categorization. AWS has no insight into the sensitivity of customer data, and must consequently treat all customer data as sensitive. As such, only a customer can determine whether data has been spilled on an EC2 instance, an EBS volume or S3 object.]* |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures

The organization:

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

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security | |
| Parameter MA-1(a): AWS Security | |
| Parameter MA-1(b)(1): [TBD by Customer] | |
| Parameter MA-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  [AWS develops, disseminates, and reviews/updates a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  [AWS has developed formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. Processes and procedures are reviewed annually.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MA-2 Controlled Maintenance

The organization:

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

| MA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance Manager | |
| Parameter MA-2(c): Data center techs | |
| Parameter MA-2(f): records in InfraDB | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MA-3 Maintenance Tools

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

| MA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance 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 | |

| MA-3 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### MA-3 (1) Control Enhancement

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: AWS Security Assurance 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 | |

| MA-3 (1) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### MA-3 (2) Control Enhancement

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: AWS Security Assurance 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 | |

| MA-3 (2) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### MA-3 (3) Control Enhancement

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

1. Verifying that there is no organizational information contained on the equipment;
2. Sanitizing or destroying the equipment;
3. Retaining the equipment within the facility; or
4. Obtaining an exemption from [FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility].

| MA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance Manager | |
| Parameter MA-3(3)(d): the information 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 | |

| MA-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MA-4 Nonlocal Maintenance

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| MA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance 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 | |

| MA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### MA-4 (2) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MA-4 (2) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MA-5 Maintenance Personnel

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

| MA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance 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 | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### MA-5 (1) Control Enhancement

The organization:

1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

| MA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security Assurance 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 | |

| MA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MA-6 Timely Maintenance

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: AWS Security Assurance Manager | |
| Parameter MA-6(1): Arbor Network’s Peakflow SP Threat Management System, Firewalls, Authlog servers, Eye of Sauron, Sauron | |
| Parameter MA-6(2): Spare parts not used. Redundant nature of architecture provides uninterrupted service. Replacement hardware is already in place in an active state. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MA-6 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
   1. Media protection policy [FedRAMP Assignment: at least annually]; and
   2. Media protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Security | |
| Parameter MP-1(a): AWS Security | |
| Parameter MP-1(b)(1): [TBD by Customer] | |
| Parameter MP-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  [AWS develops, disseminates, and reviews/updates annually a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  [AWS has developed formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MP-2 Media Access

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: AWS Physical Security Manager | |
| Parameter MP-2-1: Digital: Magnetic and non-magnetic (external hard drives, floppy disks, storage tapes, compact discs, digital video discs, USB flash/thumb drives, and diskettes)  Non-digital: Printing (Paper Output) | |
| Parameter MP-2-2: All personnel granted access to GovCloud data center facilities (via a badge swipe and PIN combination) are screened against a pre-authorized list of those needing access in order to perform their duties or are fully escorted, as appropriate. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-2 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MP-3 Media Marking

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [FedRAMP Assignment: no removable media types] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

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: AWS Physical Security Manager | |
| Parameter MP-3(b)-1: None. | |
| Parameter MP-3(b)-1: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MP-4 Media Storage

The organization:

1. Physically controls and securely stores [FedRAMP Assignment: [all types of digital and non-digital media with sensitive information]] within [FedRAMP Assignment: see additional FedRAMP requirements and guidance]; and

MP-4a Additional FedRAMP Requirements and Guidance:

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

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

| MP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter MP-4(a)-1:  Digital (Magnetic and Non-Magnetic) Media (further defined by the organization in MP-2)  Non-digital (printing output/paper) Media | |
| Parameter MP-4(a)-2: Data Centers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MP-5 Media Transport

The organization:

1. Protects and controls [FedRAMP Assignment: all media with sensitive information] during transport outside of controlled areas using [FedRAMP Assignment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container];

MP-5a Additional FedRAMP Requirements and Guidance:

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

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

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter MP-5(a)-1: Digital (Magnetic and Non-Magnetic) Media (further defined by the organization in MP-2) Non-digital (printing output/paper) Media | |
| Parameter MP-5(a)-2: : N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MP-6 Media Sanitization

The organization:

1. 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 and Section 5.9: Reuse and Disposal of Storage Media and Hardware ] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with strength and integrity commensurate with the classification or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter MP-6(a)-1: all media as referenced in MP-2 | |
| Parameter MP-6(a)-2: degaussing and/or destruction | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: AWS Physical Security Manager | |
| Parameter MP-6(2): at least quarterly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### MP-7 Media Use

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: AWS Physical Security Manager | |
| Parameter MP-7-1: See MP-2 | |
| Parameter MP-7-2: See MP-2 | |
| Parameter MP-7-3: See MP-2 | |
| Parameter MP-7-4: See MP-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 | |

| MP-7 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| MP-7 (1) is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [FedRAMP Assignment: at least 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: AWS Security | |
| Parameter PE-1(a): AWS Security | |
| Parameter PE-1(b)(1): [TBD by Customer] | |
| Parameter PE-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  [AWS has developed formal, documented physical and environmental protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy is reviewed on an annual basis.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  [AWS has developed formal, documented physical and environmental protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy is reviewed on an annual basis.]  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-2 Physical Access Authorizations

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least every ninety (90) days]; and
4. Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-2(c): at least every 90 days | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-3 Physical Access Control

The organization:

1. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by:
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];
2. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [Assignment: organization-defined physical access devices] every [FedRAMP Assignment: at least annually]; and
7. Changes combinations and keys [FedRAMP Assignment: at least annually] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-3(a): restricted areas | |
| Parameter PE-3(b): Lenel access system and security guards | |
| Parameter PE-3(c): restricted areas | |
| Parameter PE-3(d): in all circumstances within restricted access area where the information system resides | |
| Parameter PE-3(f): Lenel access system | |
| Parameter PE-3(f)-2: at least annually | |
| Parameter PE-3(g): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-4 Access Control for Transmission Medium

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: AWS Physical Security Manager | |
| Parameter PE-4-1: server rooms and assets | |
| Parameter PE-4-2: badge and PIN | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-4 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-5 Access Control for Output Devices

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-5 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-6 Monitoring Physical Access

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [FedRAMP Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

| PE-6 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-6(b)-1: daily | |
| Parameter PE-6(b)-2: suspicious activity | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### PE-6 (1) Control Enhancement

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-6 (1) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-8 Visitor Access Records

The organization:

1. Maintains visitor access records to the facility where the information system resides for [FedRAMP Assignment: for a minimum of one (1) year]; and
2. Reviews visitor access records [FedRAMP Assignment: at least monthly]

| PE-8 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-8(a): at least one year | |
| Parameter PE-8(b): at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-9 Power Equipment and Cabling

The organization protects power equipment and power cabling for the information system from damage and destruction.

| PE-9 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-9 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-10 Emergency Shutoff

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| PE-10 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-10(b): data center electrical rooms | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-11 Emergency Power

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: AWS Physical Security Manager | |
| Parameter PE-11: transition of the information to long-term alternate power | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-11 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-12 Emergency Lighting

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-12 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-13 Fire Protection

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-13 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### PE-13 (2) Control Enhancement

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: AWS Physical Security Manager | |
| Parameter PE-13(2)-1: SOC and emergency responders | |
| Parameter PE-13(2)-2: SOC and emergency responders | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-13 (2) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### PE-13 (3) Control Enhancement

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-13 (3) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-14 Temperature and Humidity Controls

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments]; and

PE-14 (a) Additional FedRAMP Requirements and Guidance:   
Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

1. Monitors temperature and humidity levels [FedRAMP Assignment: continuously].

| PE-14 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-14(a): Consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments. | |
| Parameter PE-14(b): continuously | |
| Parameter PE-14(b) Additional: The service provider measures temperature at server inlets and humidity levels by dew point. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### PE-14 (2) Control Enhancement

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-14 (2) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-15 Water Damage Protection

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: AWS Physical Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-15 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-16 Delivery and Removal

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: AWS Physical Security Manager | |
| Parameter PE-16: all information system components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PE-16 What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PE-17 Alternate Work Site

The organization:

1. Employs [Assignment: organization-defined security controls] at alternate work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| PE-17 | Control Summary Information |
| --- | --- |
| Responsible Role: AWS Physical Security Manager | |
| Parameter PE-17(a): Refer to the management, operational, and technical information system security controls for alternate work sites below in part 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 | |

| PE-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures

The organization:

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

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PL-1(a): [TBD by Customer] | |
| Parameter PL-1(b)(1): [TBD by Customer] | |
| Parameter PL-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PL-2 System Security Plan

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
3. Reviews the security plan for the information system [FedRAMP Assignment: at least annually];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PL-2(b): [TBD by Customer] | |
| Parameter PL-2(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing an SSP for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing an SSP for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing an SSP for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for developing an SSP for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for developing an SSP for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Parameter PL-2(3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PL-2 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for planning and coordinating security-related activities affecting the information system.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PL-4 Rules of Behavior

The organization:

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

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PL-4(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing rules of behavior for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing rules of behavior for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing rules of behavior for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for developing rules of behavior for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PL-4 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for developing rules of behavior for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PL-8 Information Security Architecture

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. Reviews and updates the information security architecture [FedRAMP Assignment: at least annually 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-7.

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

| PL-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PL-8(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PL-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing an SSP that properly documents the security architecture of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing an SSP that properly documents the security architecture of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing an SSP that properly documents the security architecture of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy [FedRAMP Assignment: at least annually]; and
   2. Personnel security procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PS-1(a): [TBD by Customer] | |
| Parameter PS-1(b)(1): [TBD by Customer] | |
| Parameter PS-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-2 Position Risk Designation

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [FedRAMP Assignment: at least annually].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PS-2(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for establishing risk designations along with screening criteria for the positions held by their employees and contractors that access their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for establishing risk designations along with screening criteria for the positions held by their employees and contractors that access their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for establishing risk designations along with screening criteria for the positions held by their employees and contractors that access their systems running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-3 Personnel Screening

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [FedRAMP Assignment: For national security clearances; a reinvestigation is required during the 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: [TBD by Customer] | |
| Parameter PS-3(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly screening personnel prior to granting access to their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for re screening personnel at a frequency determined by the applicable risk designations.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### PS-3 (3) Control Enhancement

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

1. Have valid access authorizations that are demonstrated by assigned official government duties; and
2. Satisfy [FedRAMP Assignment: personnel screening criteria – as required by specific information].

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

| PS-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly screening personnel prior to granting access to their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly screening personnel prior to granting access to their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-4 Personnel Termination

The organization, upon termination of individual employment:

1. Disables information system access within [FedRAMP Assignment: eight (8) hours];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PS-4(a): [TBD by Customer] | |
| Parameter PS-4(c): [TBD by Customer] | |
| Parameter PS-4(f)-1: [TBD by Customer] | |
| Parameter PS-4(f)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly terminating access for personnel to whom they have granted access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly terminating access for personnel to whom they have granted access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for conducting exit interviews that include organization-defined information security topics.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for retrieving all security-related organizational information system-related property.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for retaining access to organizational information and information systems formerly controlled by terminated individual.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for notifying organization-defined personnel within a time period defined by the organization following termination actions.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-5 Personnel Transfer

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [FedRAMP Assignment: twenty-four (24) hours];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [Assignment: organization-defined personnel or roles] within [FedRAMP Assignment: twenty-four (24) hours].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PS-5(b)-1: [TBD by Customer] | |
| Parameter PS-5(b)-2: [TBD by Customer] | |
| Parameter PS-5(d)-1: [TBD by Customer] | |
| Parameter PS-5(d)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing a personnel transfer process that satisfied these control requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing a personnel transfer process that satisfied these control requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing a personnel transfer process that satisfied these control requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for implementing a personnel transfer process that satisfied these control requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-6 Access Agreements

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [FedRAMP Assignment: at least annually]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [FedRAMP Assignment: at least annually and any time there is a change to the user's level of access].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PS-6(b): [TBD by Customer] | |
| Parameter PS-6(c)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for developing access agreements for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing access agreements for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for developing access agreements for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-7 Third-Party Personnel Security

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [FedRAMP Assignment: terminations: immediately; transfers: within twenty-four (24) hours]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter PS-7(d)-1: [TBD by Customer] | |
| Parameter PS-7(d)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for managing any third-party security personnel to whom they grant access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for managing any third-party security personnel to whom they grant access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for managing any third-party security personnel to whom they grant access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for managing any third-party security personnel to whom they grant access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for managing any third-party security personnel to whom they grant access.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### PS-8 Personnel Sanctions

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. 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: [TBD by Customer] | |
| Parameter PS-8(b)-1: [TBD by Customer] | |
| Parameter PS-8(b)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| PS-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for employing formal sanctions when personnel fails to comply with established security policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for employing formal sanctions when personnel fails to comply with established security policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [FedRAMP Assignment: at least annually]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter RA-1(a): [TBD by Customer] | |
| Parameter RA-1(b)(1): [TBD by Customer] | |
| Parameter RA-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### RA-2 Security Categorization

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly categorizing their systems hosted on AWS in accordance with FIPS 199.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly categorizing their systems hosted on AWS in accordance with FIPS 199.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly categorizing their systems hosted on AWS in accordance with FIPS 199.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### RA-3 Risk Assessment

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [Selection: security plan; risk assessment report; [FedRAMP Assignment: security assessment report]];
3. Reviews risk assessment results [FedRAMP Assignment: at least annually or whenever a significant change occurs];
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

RA-3 Additional FedRAMP Requirements and Guidance:

Requirement: Include all Authoring Officials and FedRAMP ISSOs.

1. Updates the risk assessment [FedRAMP Assignment: annually] 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 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter RA-3(b): [TBD by Customer] | |
| Parameter RA-3(c): [TBD by Customer] | |
| Parameter RA-3(d): [TBD by Customer] | |
| Parameter RA-3(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for conducting risk assessments of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for conducting risk assessments of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for conducting risk assessments of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for conducting risk assessments of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for conducting risk assessments of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### RA-5 Vulnerability Scanning

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

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

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

1. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery], in accordance with an organizational assessment of risk; and
4. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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

Requirement: To include the Risk Executive; for JAB authorizations to include FedRAMP ISSOs.

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter RA-5(a): [TBD by Customer] | |
| Parameter RA-5(d): [TBD by Customer] | |
| Parameter RA-5(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### RA-5 (1) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS with tools that are capable of being updated, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### RA-5 (2) Control Enhancement

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: [TBD by Customer] | |
| Parameter RA-5(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS and updating the list of vulnerabilities scanned, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### RA-5 (3) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for developing vulnerability scanning procedures for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### RA-5 (5) Control Enhancement

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: [TBD by Customer] | |
| Parameter RA-5(5)-1: [TBD by Customer] | |
| Parameter RA-5(5)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 (5) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### RA-5 (6) Control Enhancement

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

RA-5(6) Additional FedRAMP Requirements and Guidance:

Guidance: Include in Continuous Monitoring ISSO digest/report to JAB/AO.

| RA-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 (6) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### RA-5 (8) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| RA-5 (8) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting vulnerability scanning of their systems hosted on AWS, as well as for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website:  <https://aws.amazon.com/security/penetration-testing/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter SA-1(a): [TBD by Customer] | |
| Parameter SA-1(b)(1): [TBD by Customer] | |
| Parameter SA-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-2 Allocation of Resources

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for establishing the information security requirements for their systems hosted on AWS and allocating sufficient resources to protect their systems.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for establishing the information security requirements for their systems hosted on AWS and allocating sufficient resources to protect their systems.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for establishing the information security requirements for their systems hosted on AWS and allocating sufficient resources to protect their systems.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-3 System Development Life Cycle

The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SA-3(a): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for creating an SDLC for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for creating an SDLC for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for creating an SDLC for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for creating an SDLC for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-4 Acquisition Process

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

Additional FedRAMP Requirements and Guidance:

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

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

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  [AWS customers are responsible for creating an acquisitions process for the components of the system they deploy in AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-4 (1) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for providing a description of the functional properties of the security controls to be employed.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-4 (2) Control Enhancement

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: [TBD by Customer] | |
| Parameter SA-4-1: [TBD by Customer] | |
| Parameter SA-4-2: [TBD by Customer] | |
| Parameter SA-4-3: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-4 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for creating a design and implementation description of the functional properties of the security controls to be employed an acquisitions process for their organization.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-4 (8) Control Enhancement

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: [TBD by Customer] | |
| Parameter SA-4(8): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-4 (8) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for establishing a continuous monitoring program for their system deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-4 (9) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-4 (9) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for identifying the ports protocols and services that will be deployed with their system running on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-4 (10) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
| *[Implementation of PIV authentication capability is the responsibility of the customer. AWS provides federation capabilities that can be used by the customer to integrate their AWS and IAM accounts with their on-premise authentication store in order to meet PIV compliance standards.]* |

### SA-5 Information System Documentation

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SA-5(c): [TBD by Customer] | |
| Parameter SA-5(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for reviewing online user and administration documentation posted by AWS on its website:*  <https://aws.amazon.com/documentation/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for reviewing online user and administration documentation posted by AWS on its website:*  <https://aws.amazon.com/documentation/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for reviewing online user and administration documentation posted by AWS on its website:*  <https://aws.amazon.com/documentation/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  *[AWS customers are responsible for reviewing online user and administration documentation posted by AWS on its website:*  <https://aws.amazon.com/documentation/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  *[AWS customers are responsible for reviewing online user and administration documentation posted by AWS on its website:*  <https://aws.amazon.com/documentation/>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-8 Security Engineering Principles

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-8 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing security engineering principles within their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-9 External Information System Services

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide  
https://www.fedramp.gov/resources/documents

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SA-9(a): [TBD by Customer] | |
| Parameter SA-9(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-9 (1) Control Enhancement

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

| SA-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SA-9(1)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-9 (2) Control Enhancement

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: [TBD by Customer] | |
| Parameter SA-9(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-9 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-9 (4) Control Enhancement

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: [TBD by Customer] | |
| Parameter SA-9(4)-1: [TBD by Customer] | |
| Parameter SA-9(4)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-9 (4) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-9 (5) Control Enhancement

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: [TBD by Customer] | |
| Parameter SA-9(5)-1: [TBD by Customer] | |
| Parameter SA-9(5)-2: [TBD by Customer] | |
| Parameter SA-9(5)-3: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-9 (5) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for ensuring the compliance of any external information system services they utilize in conjunction with their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-10 Developer Configuration Management

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [FedRAMP Selection: development, implementation, AND operation];
2. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

SA-10 (e) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP ISSOs.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SA-10(a): [TBD by Customer] | |
| Parameter SA-10(b): [TBD by Customer] | |
| Parameter SA-10(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for implementing developer configuration management for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for implementing developer configuration management for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for implementing developer configuration management for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for implementing developer configuration management for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for implementing developer configuration management for their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-10 (1) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-10 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring the integrity of any software they deploy within their AWS environment.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SA-11 Developer Security Testing and Evaluation

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SA-11(b)-1: [TBD by Customer] | |
| Parameter SA-11(b)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-11 (1) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-11 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for ensuring that developers employ static code tools to identify flaws in their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-11 (2) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-11 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SA-11 (8) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SA-11 (8) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for conducting security testing and evaluation of their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter SC-1(a): [TBD by Customer] | |
| Parameter SC-1(b)(1): [TBD by Customer] | |
| Parameter SC-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-2 Application Partitioning

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-2 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for separating general user access to their systems hosted on AWS through proper implementation of the IAM service, as well as for any user accounts created within virtual machines hosted on EC2, to include customer-facing web applications.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-4 Information in Shared Resources

The information system prevents unauthorized and unintended information transfer via shared system resources.

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

| SC-4 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for protecting their data hosted on AWS to prevent disclosure, to include proper implementation of access control, networking controls and encryption.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-5 Denial of Service Protection

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: [TBD by Customer] | |
| Parameter SC-5-1: [TBD by Customer] | |
| Parameter SC-5-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-5 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for architecting highly available, durable systems on AWS, to include the implementation of documented anti-DDoS measures:*  https://d0.awsstatic.com/whitepapers/DDoS\_White\_Paper\_June2015.pdf  *Fault tolerance and high availability:*  <http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-6 Resource Availability

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: [TBD by Customer] | |
| Parameter SC-6-1: [TBD by Customer] | |
| Parameter SC-6-2: [TBD by Customer] | |
| Parameter SC-6-3: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-6 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for architecting highly available, durable systems on AWS, to include the implementation of appropriate system resource allocations*]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-7 Boundary Protection

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SC-7(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for properly implementing boundary protection mechanisms including VPC’s security groups and network ACLs.*  [*https://aws.amazon.com/whitepapers/aws-security-best-practices/*](https://aws.amazon.com/whitepapers/aws-security-best-practices/)  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for properly implementing boundary protection mechanisms including VPC’s security groups and network ACLs.*  [*https://aws.amazon.com/whitepapers/aws-security-best-practices/*](https://aws.amazon.com/whitepapers/aws-security-best-practices/)  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for properly implementing boundary protection mechanisms including VPC’s security groups and network ACLs.*  [*https://aws.amazon.com/whitepapers/aws-security-best-practices/*](https://aws.amazon.com/whitepapers/aws-security-best-practices/)  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html>]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (3) Control Enhancement

The organization limits the number external network connections to the information system.

| SC-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (3) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs to limit external network connections.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (4) Control Enhancement

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter SC-7(4)(e): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (5) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (7) Control Enhancement

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: AWS Information Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (7) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing remote connections to prevent establishing a connection to the system VPC’s security groups deployed on AWS and other system outside of the boundary. This is commonly referred to as ‘split tunneling’.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (8) Control Enhancement

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: [TBD by Customer] | |
| Parameter SC-7(8)-1: [TBD by Customer] | |
| Parameter SC-7(8)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (8) What is the solution and how is it implemented? |
| --- |
| Application  [It is a customer responsibility to route this traffic through authenticated proxy servers. This can be implemented with an EC2 instance acting as a proxy. Traffic can also be routed through a site-to-site VPN connection between the customers VPC to the customers network infrastructure and out to the internet through their existing TIC or internet proxy.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (12) Control Enhancement

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: [TBD by Customer] | |
| Parameter SC-7(12)-1: [TBD by Customer] | |
| Parameter SC-7(12)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing host-based boundary protections on their EC2 instances.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (13) Control Enhancement

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 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: [TBD by Customer] | |
| Parameter SC-7(13): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (13) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-7 (18) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing VPC’s security groups and network ACLs.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-8 Transmission Confidentiality and Integrity

The information system protects the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

| SC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SC-8: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-8 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for protecting the confidentiality and integrity of the connectivity to their EC2 systems running on AWS by installing and managing FIPS 140-2 validated software modules to handle customer connections to web applications.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-8 (1) Control Enhancement

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: [TBD by Customer] | |
| Parameter SC-8 (1)-1: [TBD by Customer] | |
| Parameter SC-8 (1)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-8 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for protecting the confidentiality and integrity of the connectivity to their EC2 systems running on AWS by installing and managing FIPS 140-2 validated software modules to handle customer connections to web applications.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-10 Network Disconnect

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: AWS Information Security Manager | |
| Parameter SC-10: no longer than 10 minutes in-band management and no longer than 15 minutes for user sessions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-10 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing network disconnects at the end of a session or after a period of inactivity.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-12 Cryptographic Key Establishment and Management

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: [TBD by Customer] | |
| Parameter SC-12: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-12 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for creating, managing and escrowing the keys they use on AWS, or choosing to use server-side encryption with keys managed by AWS. AWS customers can use AWS provided functionality such as Cloud HSM or KMS to manage their keys, or manage them using a solution of their own.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-12 (2) Control Enhancement

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: [TBD by Customer] | |
| Parameter SC-12 (2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-12 (2) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers may leverage the AWS KMS or HSM to escrow their keys, or implement an on-premise solution for escrow.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-12 (3) Control Enhancement

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: [TBD by Customer] | |
| Parameter SC-12 (3): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-12 (3) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for creating, managing and escrowing their own keys on AWS, or choosing to use server-side encryption with keys managed by AWS. AWS customers can use AWS provided functionality such as Cloud HSM or KMS to manage their keys, or manage them using a solution of their own.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-13 Cryptographic Protection

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: [TBD by Customer] | |
| Parameter SC-13: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-13 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for implementing FIPS validated or NSA approved encryption modules within their applications and guest operating systems.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-15 Collaborative Computing Devices

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[FedRAMP Assignment: no exceptions] and
2. Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SC-15(a): no exceptions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for implement safeguards that prevent the remote activation of collaborative computing devices and providing explicit indication to users when in use.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for implement safeguards that prevent the remote activation of collaborative computing devices and providing explicit indication to users when in use.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Application  *[AWS customers are responsible for implement safeguards that prevent the remote activation of collaborative computing devices and providing explicit indication to users when in use.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-17 Public Key Infrastructure Certificates

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: [TBD by Customer] | |
| Parameter SC-17: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-17 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for obtaining certificates from an approved certificate authority.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-18 Mobile Code

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for developing and enforcing a mobile code policy.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for developing and enforcing a mobile code policy.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[AWS customers are responsible for developing and enforcing a mobile code policy.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-19 Voice Over Internet Protocol

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for developing VoIP policies and implementation guidance if it is in use on their system hosted on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for developing VoIP policies and implementation guidance if it is in use on their system hosted on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-20 Secure Name / Address Resolution Service (Authoritative Source)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[AWS customers are responsible for any DNS services they implement within their systems hosted on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[AWS customers are responsible for any DNS services they implement within their systems hosted on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-21 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for any DNS services they implement within their systems hosted on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-22 Architecture and Provisioning for Name / Address Resolution Service

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-22 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for any DNS services they implement within their systems hosted on AWS.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-23 Session Authenticity

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-23 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers are responsible for ensuring session authenticity for any connections to web applications they install on their AWS workloads.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-28 Protection of Information at Rest

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: [TBD by Customer] | |
| Parameter SC-28-1: [TBD by Customer] | |
| Parameter SC-28-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-28 What is the solution and how is it implemented? |
| --- |
| Application  *[Amazon S3 supports several mechanisms that provide users flexibility to control access of data at rest as well as how, when, and where they can access it. Amazon S3 also provides options for encryption of data at rest. Users can also encrypt data prior to uploading to S3. Alternately, users can employ S3 Server Side Encryption (SSE) which uses AES-256 encryption. With S3 SSE, customers can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved. AWS customers may also chose to implement client-side encryption.*  [*http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html*](http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html)*]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SC-28 (1) Control Enhancement

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: [TBD by Customer] | |
| Parameter SC-28(1)-1: [TBD by Customer] | |
| Parameter SC-28(1)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-28 (1) What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers can encrypt data prior to uploading to S3. Alternately, customers can employ S3 Server Side Encryption (SSE) or EBS SSE which uses AES-256 encryption. With S3 SSE or EBS SSE, customers can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved. Mission owners can also use their own encryption keys with the Amazon S3 server-side encryption feature.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SC-39 Process Isolation

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SC-39 What is the solution and how is it implemented? |
| --- |
| Application  *[AWS customers should use modern operating systems that support creating separate execution domains for each process.]*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
   1. System and information integrity policy [FedRAMP Assignment: at least 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: [TBD by Customer] | |
| Parameter SI-1(a): [TBD by Customer] | |
| Parameter SI-1(b)(1): [TBD by Customer] | |
| Parameter SI-1(b)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  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 | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for developing policies and procedures that apply specifically to the application]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-2 Flaw Remediation

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [FedRAMP Assignment: thirty 30 days of release of updates] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-2(c): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for remediating vulnerabilities within their systems hosted on AWS in accordance with the timelines associated with the severity of the vulnerability.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for remediating vulnerabilities within their systems hosted on AWS in accordance with the timelines associated with the severity of the vulnerability.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for remediating vulnerabilities within their systems hosted on AWS in accordance with the timelines associated with the severity of the vulnerability.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for remediating vulnerabilities within their systems hosted on AWS in accordance with the timelines associated with the severity of the vulnerability.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-2 (2) Control Enhancement

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: [TBD by Customer] | |
| Parameter SI-2 (2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-2 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for performing operating system vulnerability scanning, web application, and database scanning (as applicable) for assets for which they have implementation responsibility (above the hypervisor).]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-2 (3) Control Enhancement

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

| SI-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-2(3)(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-2 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for flaw identification and flaw remediation within their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for flaw identification and flaw remediation within their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-3 Malicious Code Protection

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [FedRAMP Assignment: to include blocking and quarantining malicious code and alerting administrator or defined security personnel near-real-time] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-3(c)(1)-1: [TBD by Customer] | |
| Parameter SI-3(c)(1)-2: [TBD by Customer] | |
| Parameter SI-3(c)(2): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-3 (1) Control Enhancement

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-3 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-3 (2) Control Enhancement

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-3 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-3 (7) Control Enhancement

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-3 (7) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for deploying, updating and managing anti-malware mechanisms on their AWS workloads, in accordance with their organization’s anti-malware policies and procedures.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-4 Information System Monitoring

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
3. Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

| SI-4 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-4(a)(1): [TBD by Customer] | |
| Parameter SI-4(b): [TBD by Customer] | |
| Parameter SI-4(g)-1: [TBD by Customer] | |
| Parameter SI-4(g)-2: [TBD by Customer] | |
| Parameter SI-4(g)-3: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part e | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part f | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part g | Application  *[*AWS customers *are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.*  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (1) Control Enhancement

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring alerts and identifying unauthorized use of information systems]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (2) Control Enhancement

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (2) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing automated monitoring tools and monitoring alerts and identifying unauthorized use of information systems]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (4) Control Enhancement

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: [TBD by Customer] | |
| Parameter SI-4(4): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring inbound and outbound communications traffic for their workloads deployed on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (5) Control Enhancement

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: [TBD by Customer] | |
| Parameter SI-4(5)-1: [TBD by Customer] | |
| Parameter SI-4(5)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (5) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for implementing monitoring tools on their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (14) Control Enhancement

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: AWS Information Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
| Inherited from pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (16) Control Enhancement

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for correlating information from monitoring tools employed throughout their systems hosted on AWS.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-4 (23) Control Enhancement

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: [TBD by Customer] | |
| Parameter SI-4(23)-1: [TBD by Customer] | |
| Parameter SI-4(23)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-4 (23) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for the implementation and management of host-based monitoring systems on their AWS workloads.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-5 Security Alerts, Advisories, and Directives

The organization:

1. Receives information system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

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

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for monitoring security alerts and advisories and taking appropriate action as required by this control.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for monitoring security alerts and advisories and taking appropriate action as required by this control.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for monitoring security alerts and advisories and taking appropriate action as required by this control.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for monitoring security alerts and advisories and taking appropriate action as required by this control.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-6 Security Functionality Verification

The information system:

1. Verifies the correct operation of [Assignment: organization-defined security functions];
2. Performs this verification [FedRAMP Assignment: to include upon system startup and/or restart at least monthly];
3. Notifies [FedRAMP Assignment: to include system administrators and security personnel] of failed security verification tests; and
4. [Selection (one or more): shuts the information system down; restarts the information system; [FedRAMP Assignment: to include notification of system administrators and security personnel] when anomalies are discovered.

| SI-6 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-6(a): [TBD by Customer] | |
| Parameter SI-6(b): [TBD by Customer] | |
| Parameter SI-6(c): [TBD by Customer] | |
| Parameter SI-6(d)-1: [TBD by Customer] | |
| Parameter SI-6(d)-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part c | Application  [AWS customers are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part d | Application  [AWS customers are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-7 Software, Firmware, and Information Integrity

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: [TBD by Customer] | |
| Parameter SI-7: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-7 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring and detecting unauthorized changes to software and information within their information system as well as assessing the integrity of software and information by performing integrity scans of the information system at least monthly.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-7 (1) Control Enhancement

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: [TBD by Customer] | |
| Parameter SI-7(1)-1: [TBD by Customer] | |
| Parameter SI-7(1)-2: [TBD by Customer] | |
| Parameter SI-7(1)-3: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for monitoring and detecting unauthorized changes to software and information within their information system as well as assessing the integrity of software and information by performing integrity scans of the information system.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

#### SI-7 (7) Control Enhancement

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: [TBD by Customer] | |
| Parameter SI-7 (7): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-7 (7) What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for incorporating detection of unauthorized changes into their incident response capabilities.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-8 Spam Protection

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

| SI-8 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | *[If the customer uses the System to host e-mail capabilities, it is the customer’s responsibility to employ the appropriate levels of spam protection at e-mail entry and exit points and to update spam definitions when new releases are made available.]* |
| Part b | *[If the customer uses the System to host e-mail capabilities, it is the customer’s responsibility to employ the appropriate levels of spam protection at e-mail entry and exit points and to update spam definitions when new releases are made available.]* |

#### SI-8 (1) Control Enhancement

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-8 (1) What is the solution and how is it implemented? |
| --- |
| *[If the customer uses the System to host e-mail capabilities, it is the customer’s responsibility to employ the appropriate levels of spam protection at e-mail entry and exit points and to update spam definitions when new releases are made available.]* |

#### SI-8 (2) Control Enhancement

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-8 (2) What is the solution and how is it implemented? |
| --- |
| *[If the customer uses the system to host e-mail capabilities, it is the customer’s responsibility to employ the appropriate levels of spam protection at e-mail entry and exit points and to update spam definitions when new releases are made available. ]* |

### SI-10 Information Input Validation

The information system checks the validity of [Assignment: organization-defined information inputs].

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-10: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-10 What is the solution and how is it implemented? |
| --- |
| Application  [Customers using S3 or EBS should develop a policy identifying acceptable data types to be stored. The customer is also responsible for defining field types, creating input validation rules for specific objects, as well as configuring any input restrictions and conducting any validity checks required. In addition, the customer is responsible for ensuring only authorized individuals are designated as administrators within the management portal.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-11 Error Handling

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [Assignment: organization-defined personnel or roles].

| SI-11 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-11(b): [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Application  [AWS customers are responsible for reviewing error messages received from AWS, as well as generating error messages as appropriate within any workloads deployed on the AWS infrasturcture.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |
| Part b | Application  [AWS customers are responsible for reviewing error messages received from AWS, as well as generating error messages as appropriate within any workloads deployed on the AWS infrasturcture.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-12 Information Handling and Retention

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: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-12 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly handling and retaining their data in accordance with the applicable applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

### SI-16 Memory Protection

The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: [TBD by Customer] | |
| Parameter SI-16-1: [TBD by Customer] | |
| Parameter SI-16-2: [TBD by Customer] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| Application  [AWS customers are responsible for properly implementing their EC2 instances in accordance with their organization’s relevant Windows or Linux hardening policies.]  Infrastructure  Reference the pre-existing FedRAMP [Provisional OR Agency] Authorization to Operate for [AWS Region], [Date of Authorization]. |

# Acronyms

| Acronym | Definition |
| --- | --- |
| 3PAO | Third Party Assessment Organization |
| AC | Access Control (Table 13 1 Summary of Required Security Controls) |
| AO | Authorizing Official |
| ASHRAE | American Society of Heating, Refrigerating and Air-conditioning Engineers (PE-14 Temperature and Humidity Controls) |
| AT | Awareness and Training (Table 13 1 Summary of Required Security Controls) |
| ATO | Authority To Operate |
| AU | Audit and Accountability (Table 13 1 Summary of Required Security Controls) |
| CONOPS | Concept Of Operations [PL-8] |
| CA | Security Assessment and Authorization (Table 13 1 Summary of Required Security Controls) |
| CERT | Computer Emergency Response Team |
| CIRT | Consumer Incident Response Team |
| CIS | Control Implementation Summary |
| CM | Configuration Management (Table 13 1 Summary of Required Security Controls) |
| CMVP | Cryptographic Module Validation Program |
| CP | Contingency Planning (Table 13 1 Summary of Required Security Controls) |
| CSP | Cloud Service Provider |
| CUI | Confidential Unclassified Information |
| DAA | Designated Approving Authority |
| DMZ | Demilitarized Zones [SC-7 (13)] |
| DNS | Domain Name System |
| DoD | Department of Defense |
| DHS | Department of Homeland Security |
| E-Authentication | Electronic Authentication |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standard |
| GSA | General Services Administration |
| HIDS | Host Intrusion Detection System |
| HIPAA | Health Insurance Portability and Accountability Act |
| HIPS | Host Intrusion Prevention System |
| HTTP | Hyper Text Transport Protocol |
| IA | Identification and Authentication (Table 13 1 Summary of Required Security Controls) |
| IAP | Internet Access Points [SC-7 (13)] |
| IaaS | Infrastructure as a Service |
| IPSec | Internet Protocol Security (Table 11-1) |
| IR | Incident Response (Table 13 1 Summary of Required Security Controls) |
| ISPP | Information Security Policies and Procedures |
| ISSO | Information System Security Officer |
| JAB | Joint Authorization Board |
| MA | Maintenance (Table 13 1 Summary of Required Security Controls) |
| MP | Media Protection (Table 13 1 Summary of Required Security Controls) |
| NARA | National Archives and Records Administration |
| NIAP | National Information Assurance Partnership [IA-2 (11)] |
| NIST | National Institute of Standards and Technology |
| NIST-SP | NIST Special Publication |
| NLA | No Logical Access (Table 9‑1 Personnel Roles and Privileges) |
| NP | Non-Privileged (Table 9‑1 Personnel Roles and Privileges) |
| OMB | Office of Management and Budget |
| P | Privileged (Table 9‑1 Personnel Roles and Privileges) |
| PaaS | Platform as a Service |
| P-ATO | Provisional Authorization to Operate |
| PDS | Protective Distribution System [SC-8 (1)] |
| PE | Physical and Environmental Protection (Table 13 1 Summary of Required Security Controls) |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure [SC-7 (13)] |
| PL | Planning (Table 13 1 Summary of Required Security Controls) |
| PMO | Program Management Office [CA-2 Security Assessments] |
| POA&M | Plan Of Action & Milestones [CA-5, CA-7] |
| PS | Personnel Security (Table 13 1 Summary of Required Security Controls) |
| PTA | Privacy Threshold Analysis |
| RA | Risk Assessment (Table 13 1 Summary of Required Security Controls) |
| RoB | Rules of Behavior |
| SA | System and Services Acquisition (Table 13 1 Summary of Required Security Controls) |
| SaaS | Software as a Service |
| SAP | Security Assessment Plan |
| SAR | Security Assessment Report |
| SC | System and Communications Protection (Table 13 1 Summary of Required Security Controls) |
| SI | System and Information Integrity (Table 13 1 Summary of Required Security Controls) |
| SLA | Service Level Agreement [CP-2 (4), CP-9 (5), CP-10 (4)] |
| SOC | Security Operations Center |
| SP | Service Processor (Table 11‑1 System Interconnections) |
| SSL | Secure Sockets Layer (Table 11‑1 System Interconnections) |
| SSP | System Security Plan |
| TCP | Transmission Control Protocol |
| US-CERT | U.S. Computer Emergency Response Team [IR-4 (8), IR-6, SI-4, SI-5] |
| UDP | User Diagram Protocol |
| VPN | Virtual Private Network (Table 11‑1 System Interconnections) |

SYSTEM SECURITY PLAN ATTACHMENTS

Instruction: Attach any additional documents that are referred to in the Information System Name (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.

# Attachments

A recommended attachment file naming convention is provided in Table 15‑1 Attachment File Naming Convention. Use this to generate names for the attachment files and to use in the Revision History tables that appear throughout this section. 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 the additional documents using the “xx” portion of the File Name. Example Information System Abbreviation A1 ISP xx v1.0. Delete the “xx” if there is only one attachment.
* 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. In this table, it is a place-holder to show you where to enter Version Number in the File Name in the Revision History tables throughout this section.

Table ‑. Attachment File Naming Convention

|  |  |  |
| --- | --- | --- |
| Attachment | File Name | File Extension |
| Information Security Policies and Procedures | Information System Abbreviation A1 ISP xx v1.0 | . enter extension |
| User Guide | Information System Abbreviation A2 UG v1.0 | . enter extension |
| E-Authentication Worksheet | Information System Abbreviation A3 e-Auth v1.0 | . enter extension |
| PTA/PIA | Information System Abbreviation A4 PTA-PIA v1.0 | . enter extension |
| Rules of Behavior | Information System Abbreviation A5 ROB v1.0 | . enter extension |
| Information System Contingency Plan | Information System Abbreviation A6 ISCP v1.0 | . enter extension |
| Configuration Management Plan | Information System Abbreviation A7 CMP v1.0 | . enter extension |
| Incident Response Plan | Information System Abbreviation A8 IRP v1.0 | . enter extension |
| CIS Summary Report | Information System Abbreviation A9 CIS Report v1.0 | . enter extension |
| CIS Worksheet | Information System Abbreviation A9 CIS WSv1.0 | . enter extension |
| FIPS 199 | Information System Abbreviation A10 FIPS v1.0 | . enter extension |
| Inventory | 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. Maintain a current Revision History in the table below.

Information Security Policies and Procedures   
Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A1 ISP v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 2 - User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

User Guide Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A2 UG v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 3 – E-Authentication

All Authorization Packages must include an E-Authentication attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

The E-Authentication Template can be found on the following FedRAMP website page: <https://www.fedramp.gov/resources/templates-2016/>

The E-Authentication Template explains the objective for selecting the appropriate E-Authentication level for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 1, Electronic Authentication Guideline.

E-Authentication Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A3 e-Auth v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 4 – PTA / PIA

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

The PTA and PIA Template can be found on the following FedRAMP website page: <https://www.fedramp.gov/resources/templates-2016/>

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues.

PTA/PIA Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A4 PTA-PIA v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 5 - Rules of Behavior

All Authorization Packages must include a Rules of Behavior attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

Rules of Behavior describe controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures. Security control PL-4 requires a Cloud Service Provider (CSP) to implement Rules of Behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

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.

Rules of Behavior Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A5 ROB v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 6 – Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

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.

Information System Contingency Plan Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A6 ISCP v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 7 - Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

Configuration Management Plan Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A7 CMP v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 8 - Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

Incident Response Plan Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A8 IRP v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 9 - CIS Report and Worksheet

All Authorization Packages must include Control Implementation Summary (CIS) Report and Worksheet attachments, which will be reviewed for quality. Maintain a current Revision History in the table below.

Templates for both can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The Report Template has a sample format. The CSP may modify the format as necessary to comply with its internal policies and FedRAMP requirements.

CIS Report and Worksheet Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A9 CIS Report v1 0.ext | 1.0 | <Revision Description> |
| <Date> | Information System Abbreviation A9 CIS WS v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 10 - FIPS 199

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

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: 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 CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

The FIPS 199 Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

FIPS 199 Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A10 FIPS v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 11 - Separation of Duties Matrix

All Authorization Packages must include a Separation of Duties Matrix attachment, which will be reviewed for quality. Maintain a current Revision History in the table below.

ATTACHMENT 11 - Separation of Duties Matrix is referenced in the following controls.

AC-5 Separation of Duties Additional FedRAMP Requirements and Guidance

Separation of Duties Matrix Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A11 SOD v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments:

## ATTACHMENT 12 – FedRAMP Laws and Regulations

The Table 15‑2 FedRAMP Templates that Reference FedRAMP Laws and Regulations lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance (SSP, SAP, SAR etc.) reference this section and attachment.

Table ‑ FedRAMP Templates that Reference FedRAMP Laws and Regulations

| 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 |

### FedRAMP Applicable Laws

Current laws and regulations as applicable to each template are shown in Table 15‑3 FedRAMP Laws and Regulations.

Table ‑ FedRAMP Laws and Regulations

| FedRAMP Laws and Regulations | | | | | Applies to these Templates | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Number | Source | Title | Date | Link | SSP | SAP | SAR | PTA/PIA | ISCP | FIPS 199 |
| 44 USC 31 | US Code | Title 44 Public Printing and Documents; Chapter 31 Records Management by Federal Agencies | January 2012 | [44 USC 31](https://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap31) | x | x | x |  | x |  |
| 5 USC 552a | US Code | Title 5 Government Organization and Employees; Chapter 5 Administrative Procedure; Section 552a Records maintained on individuals (Privacy Act of 1974 as amended) | January 2014 | [5 USC 552A](https://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf) | x |  | x | x | x |  |
| HSPD-12 | Homeland Security Presidential Directive | Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors [HSPD-12], August 27, 2004 | August 2004 | [HSPD-12](http://www.dhs.gov/homeland-security-presidential-directive-12) | x |  |  |  |  | x |
| HSPD-7 | Homeland Security Presidential Directive | Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7], December 17, 2003 | December 2003 | [HSPD-7](http://www.dhs.gov/homeland-security-presidential-directive-7) | x |  | x |  | x |  |
| OMB Circular A-108 | Office of Management and Budget | Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [, as amended] | Rescinded by OMB A-130 | Archived |  | x | x |  |  |  |
| OMB Circular A-123 | Office of Management and Budget | Management’s Responsibility for Internal Control Revised | December 2004 | [OMB A-123](https://www.whitehouse.gov/omb/circulars_a123_rev/) | x |  | x |  | x |  |
| OMB Circular A-130 | Office of Management and Budget | Management of Federal Information Resources, Revised, Transmittal Memorandum No. 4 | November 2000 | [OMB A-130](https://www.whitehouse.gov/omb/circulars_a130/) | x | x | x | x | x | x |
| OMB Circular A-130 iii | Office of Management and Budget | Security of Federal Automated Information Systems, Appendix III | November 2000 | [OMB A-130 Appendix iii](https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii) | x | x | x |  | x |  |
| OMB M-01-05 | Office of Management and Budget | Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy | December 2000 | [OMB M 01-05](https://www.whitehouse.gov/omb/memoranda_m01-05/) | x | x | x |  | x |  |
| OMB M-03-22 | Office of Management and Budget | OMB Guidance for Implementing the Privacy Provisions | September 2003 | [OMB M-03-22](https://www.whitehouse.gov/omb/memoranda_m03-22) |  |  |  | x |  |  |
| OMB M-04-04 | Office of Management and Budget | E-Authentication Guidance for Federal Agencies | December 2003 | [OMB M 04-04](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf) | x |  | x |  | x | x |
| OMB M-06-16 | Office of Management and Budget | Protection of Sensitive Agency Information | June 2006 | [OMB M-06-16](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf) | x | x | x |  | x |  |
| OMB M-07-16 | Office of Management and Budget | Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII) | May 2007 | [OMB M-07-16](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf) |  |  |  | x |  |  |
| OMB M-10-23 | Office of Management and Budget | Guidance for Agency Use of Third-Party Websites | June 2010 | [OMB M-10-23](https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf) |  |  |  | x |  |  |
| OMB M-99-18 | Office of Management and Budget | Privacy Policies on Federal Web Sites | June 1999 | [OMB M-99-18](https://www.whitehouse.gov/omb/memoranda_m99-18/) |  |  |  | x |  |  |
| PL 99-474 | US Code Public Law | Computer Fraud and Abuse Act , 18 USC 1030 | October 1986 | [PL 99-474](https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1213.pdf) | x | x | x |  | x |  |
| PL 100-503 | US Code Public Law | Consolidated Appropriations Act of 2005, Section 522 | October 1988 | [PL 100-503](https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf) |  |  |  | x |  | x |
| PL 104-191 | US Code Public Law | Health Insurance Portability and Accountability Act of 1996 (HIPAA) | August 1996 | [PL 104-191](https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/hipaalaw.pdf) |  |  |  | x |  |  |
| PL 104-231 | US Code Public Law | Electronic Freedom of Information Act As Amended in 2002 [PL 104-231, 5 USC 552], October 2, 1996 | October 1996 | [PL 104-231](https://www.congress.gov/104/plaws/publ231/PLAW-104publ231.pdf) | x | x | x | x | x |  |
| PL 107-56 | US Code Public Law | USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) | October 2001 | [PL 107-56](https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf) |  |  |  |  |  | x |
| PL 107-347 | US Code Public Law | E-Government Act [includes FISMA Title III] | December 2002 | [PL 107-347](https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf) | x | x | x | x | x | x |
| PL 108-447 | US Code Public Law | Consolidated Appropriations Act of 2005, Section 522 | September 2005 | [PL 108-447](https://www.gpo.gov/fdsys/pkg/PLAW-108publ447/pdf/PLAW-108publ447.pdf) |  |  |  |  |  | x |
| PL 113-187 | US Code Public Law | 44 U.S.C The Presidential and Federal Records Act Amendments of 2014 showing changes to NARA Statutes found below in Chapters 21, 22, 29, 31, 33, of Title 44 in PDF. | December 2014 | [PL 113-187](https://www.archives.gov/about/laws/p-l-113-187.pdf) |  |  |  | x |  |  |
| NARA | National Archives | 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33 (see Public Law 113-187) | February 2008 | [NARA 44USC](https://www.archives.gov/about/laws/) |  |  |  | x |  |  |
| FTC | Federal Trade Commission | Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices | June 2008 | [FTC Sec-5](http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf) |  |  |  | x |  |  |
| NCSL | National Conference of State Legislatures | State Privacy Laws | January 2016 | [NCSL](http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx) |  |  |  |  |  | x |
| ECFR | Electronic Code of Federal Regulations | Title 35, Code of Federal Regulations, Chapter XII, Subchapter B | March 2016 | [e-CFR data](http://162.140.57.127/cgi-bin/ECFR?page=browse) |  |  |  | x |  |  |

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

### FedRAMP Applicable Standards and Guidance

Table 15‑4 FedRAMP Applicable Standards and Guidance reflects current standards and guidance as applicable to each template.

Table ‑ FedRAMP Applicable Standards and Guidance

| FedRAMP Laws and Regulations | | | | | | Applies to these Templates | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Identification Number | Source | Title | Date | Link | SSP | | SAP | SAR | PIA/PTA | ISCP | FIPS 199 |
| FIPS PUB 140-2 | Federal Information Processing Standards Publication | Security Requirements for Cryptographic Modules | May 2001 | [FIPS 140-2](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) | x | | x | x |  | x |  |
| FIPS PUB 199 | Federal Information Processing Standards Publication | Standards for Security Categorization of Federal Information and Information Systems | February 2004 | [FIPS 199](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) | x | |  | x |  | x | x |
| FIPS PUB 200 | Federal Information Processing Standards Publication | Minimum Security Requirements for Federal Information and Information Systems | March 2006 | [FIPS 200](http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf) | x | |  | x |  | x | x |
| FIPS PUB 201-2 | Federal Information Processing Standards Publication | Personal Identity Verification (PIV) of Federal Employees and Contractors | August 2013 | [FIPS 201-2](http://dx.doi.org/10.6028/NIST.FIPS.201-2) | x | | x | x |  | x | x |
| NIST SP 800-18 | National Institute of Standards and Technology | Guide for Developing Security Plans for Federal Information Systems, Revision 1 | February 2006 | [SP 800-18](http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) | x | | x | x |  | x | x |
| NIST 800-26 | National Institute of Standards and Technology | Security Self-Assessment Guide for Information Technology Systems | Superseded By: FIPS 200, SP 800-53, SP 800-53A | [Archived NIST SP](http://csrc.nist.gov/publications/PubsSPArch.html) |  | |  |  |  |  | x |
| NIST SP 800-27 | National Institute of Standards and Technology | Engineering Principles for Information Technology Security Revision A (A Baseline for Achieving Security) | June 2004 | [SP 800-27](http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf) | x | |  | x |  | x |  |
| NIST SP 800-30 | National Institute of Standards and Technology | Guide for Conducting Risk Assessments, Revision 1 | January 2015 | [SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) | x | | x | x |  | x | x |
| NIST SP 800-34 | National Institute of Standards and Technology | Contingency Planning Guide for Federal Information Systems Revision 1 [includes updates as of 11-11-10] | May 2010 | [SP 800-34](http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf) | x | | x | x |  | x | x |
| NIST SP 800-37 | National Institute of Standards and Technology | Guide for Mapping Types of Information and Information Systems to Security Categories (Revision 1) | February 2010 | [SP 800-37](http://dx.doi.org/10.6028/NIST.SP.800-37r1) | x | | x | x |  | x | x |
| NIST SP 800-39 | National Institute of Standards and Technology | Managing Information Security Risk: Organization, Mission, and Information System View | March 2011 | [SP 800-39](http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf) |  | | x | x |  | x |  |
| NIST 800-47 | National Institute of Standards and Technology | NIST 800-47, Security Guide for Interconnecting Information Technology Systems | August 2002 | [SP 800-47](http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf) |  | |  |  |  |  | x |
| NIST SP 800-53 | National Institute of Standards and Technology | Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 [Includes updates as of 01-22-2015] | April 2013 | [SP 800-53](http://dx.doi.org/10.6028/NIST.SP.800-53r4) | x | | x | x |  | x | x |
| NIST SP 800-53A | National Institute of Standards and Technology | Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Revision 4 | December 2014 | [SP 800-53A](http://dx.doi.org/10.6028/NIST.SP.800-53Ar4) | x | | x | x |  | x | x |
| NIST SP 800-60 | National Institute of Standards and Technology | Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1 | August 2008 | [SP 800-60](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf) | x | |  | x |  |  | x |
| NIST SP 800-61 | National Institute of Standards and Technology | Computer Security Incident Handling Guide, Revision 2 | August 2012 | [SP 800-61](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) | x | |  | x |  | x |  |
| NIST SP 800-63-2 | National Institute of Standards and Technology | Electronic Authentication Guideline: Computer Security, Revision 2 | August 2013 | [SP 800-63-2](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf) |  | |  |  |  |  | x |
| NIST SP 800-64 | National Institute of Standards and Technology | Security Considerations in the System Development Life Cycle, Revision 2 | October 2008 | [SP 800-64](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf) | x | | x | x |  | x | x |
| NIST SP 800-115 | National Institute of Standards and Technology | Technical Guide to Information Security Testing and Assessment | September 2008 | [SP 800-115](http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf) | x | | x | x |  | x |  |
| NIST SP 800-128 | National Institute of Standards and Technology | Guide for Security-Focused Configuration Management of Information Systems | August 2011 | [SP 800-128](http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf) | x | |  | x |  | x |  |
| NIST SP 800-137 | National Institute of Standards and Technology | Information Security Continuous Monitoring for Federal Information Systems and Organizations | September 2011 | [SP 800-137](http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf) | x | |  | x |  | x |  |
| NIST SP 800-144 | National Institute of Standards and Technology | Guidelines on Security and Privacy in Public Cloud Computing | December 2011 | [SP 800-144](http://dx.doi.org/10.6028/NIST.SP.800-144) |  | |  |  |  |  | x |
| NIST SP 800-145 | National Institute of Standards and Technology | The NIST Definition of Cloud Computing | September 2011 | [SP 800-145](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf) | x | |  | x |  | x |  |
| FTC | Federal Trade Commission | Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress | June 1998 | [FTC Privacy Online](https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission) |  | |  |  |  |  | x |
| NARA 2010-05 | National Archives NARA Bulletin 2010-05 | Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin) | September 2010 | [NARA 2010-05](http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html) |  | |  |  |  |  | x |
| FDIC | Federal Deposit Insurance Corporation | Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks | June 2004 | [FDIC Privacy Risks](https://www.fdic.gov/regulations/examinations/offshore/offshore_outsourcing_06-04-04.pdf) |  | |  |  |  |  | x |

The FedRAMP Standards and Guidance workbook can be submitted as an appendix or an attachment. The attachment can be found on this page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

Note: All NIST Computer Security Publications can be found at the following  
URL: <http://csrc.nist.gov/publications/PubsSPs.html>

Additional Comments:

## ATTACHMENT 13 – FedRAMP Inventory Workbook

All Authorization Packages must include three Inventory attachments, which will be reviewed for quality. Maintain a current Revision History in the table below.

* Prepare an Inventory listing the principal hardware components for Information System Abbreviation.
* Prepare an Inventory listing the principal software components for Information System Abbreviation.
* Prepare an Inventory listing the principal network devices and components for Information System Abbreviation.

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

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

FedRAMP Inventory Workbook Revision History

| Date | File Name and Extension | Version | Comments |
| --- | --- | --- | --- |
| <Date> | Information System Abbreviation A13 INV-H v1 0.ext | 1.0 | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |
| <Date> | <Enter revision file name and extension> | <Version> | <Revision Description> |

Additional Comments: