FedRAMP *Tailored* Low Impact

Software as a Service (LI-SaaS)   
Framework Template



Federal Risk and Authorization Management Program

CSP Name

Information System Name

Version #.#

Version Date

# Executive Summary

The purpose of this document is to provide a framework for describing the security risk posture of cloud-based Software as a Service (SaaS) applications based on the FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) security control baseline in support of risk-based decisions for granting Federal Authority to Operate (ATOs).

**Scope**

The FedRAMP *Tailored* LI-SaaSframework incorporates the following:

* General information about the application/services including system owner, Points of Contact (POC), etc.
* Descriptions of the application/service including deployment model, application/system boundary and all “component types” included in-boundary.
* Descriptions of how selected FedRAMP *Tailored* LI-SaaS baseline minimum security control requirements are implemented by the service provider.
* Descriptions of how implementation of the required security controls will be validated by the independent assessor.
* Results of the validation/assessment of the security control implementations.
* Descriptions of remediation and/or mitigation of risks identified in the validation/ assessment results.

**System, Control Implementation, and Remediation Descriptions Prepared by:**

|  |  |  |
| --- | --- | --- |
| **Identification of Organization that Prepared These Components of the Document** | | |
| <Logo> | **Organization Name** | <Company/Organization>. |
| **Street Address** | <Street Address> |
| **Suite/Room/Building** | <Suite/Room/Building> |
| **City, State Zip** | <Zip Code> |

**System, Control Implementation, and Remediation Descriptions Prepared for:**

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

**Assessment Plan/Procedures and Assessment Results Prepared by:**

|  |  |  |
| --- | --- | --- |
| **Identification of Independent Assessor** | | |
| <Logo> | **Organization Name** | <Company/Organization>. |
| **Street Address** | <Street Address> |
| **Suite/Room/Building** | <Suite/Room/Building> |
| **City, State Zip** | <Zip Code> |

Template Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Template Version** | **Author** |
| 6/19/2017 | Initial release version | 1.0 | FedRAMP PMO |
| 7/11/2017 | Updated based on first round of public comments | 2.0 | FedRAMP PMO |
| 8/23/2017 | Final baseline for publication/use | 3.0 | FedRAMP PMO |
| 8/25/2017 | Minor content revisions to more properly align with the core document | 3.2 | FedRAMP PMO |
| 9/21/2017 | Revised the SA-9 requirement statement to resolve a copy/paste error | 3.3 | FedRAMP PMO |
| 10/27/2017 | Revised AC-2 to better reflect the exclusion of some clauses. Revised SA-9 to address a copy/past error, and adds missing control CA-3. | 3.4 | FedRAMP PMO |
|  |  |  |  |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Document Version** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**How to Contact Us**

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

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

*Instructions for completing this document*

**How to Complete this Document**

Each component of the FedRAMP *Tailored* LI-SaaS Framework will be completed by the entity responsible for the information, as follows:

|  |  |
| --- | --- |
| **Framework Component** | **Entity Responsible** |
| Introductory Sections 1-12 | Application/Service Provider |
| Minimum Security Controls – Section 13 |  |
| Control Summary and Implementation Descriptions | Application/Service Provider |
| Assessment Plan/Procedures | Independent Assessor |
| Assessment Results | Independent Assessor |
| Remediation Plan | Application/Service Provider |
| Summary Table of Risks | Independent Assessor |
| Summary Table of Remediation Plans | Application/Service Provider |
| List of Attachments | Application/Service Provider and Independent Assessor as applicable |

*Remove all instructions from your final version of the document.*

Table of Contents

[Executive Summary i](#_Toc496867014)

[1. Information System Name 1](#_Toc496867015)

[2. Information System Categorization 1](#_Toc496867016)

[2.1. Information Types 1](#_Toc496867017)

[2.2. Security Objectives Categorization (FIPS 199) 3](#_Toc496867018)

[3. Information System Owner 4](#_Toc496867019)

[4. Independent Assessor 4](#_Toc496867020)

[5. Authorizing Official 4](#_Toc496867021)

[6. Other Designated Contacts 5](#_Toc496867022)

[7. Assignment of Security Responsibility 6](#_Toc496867023)

[8. Information System Operational Status 6](#_Toc496867024)

[9. Information System Type 7](#_Toc496867025)

[9.1. Cloud Service Models 7](#_Toc496867026)

[9.2. Cloud Deployment Models 8](#_Toc496867027)

[9.3. Leveraged Authorizations 8](#_Toc496867028)

[10. General System Description 9](#_Toc496867029)

[10.1. System Function or Purpose 9](#_Toc496867030)

[10.2. Information System Components and Boundaries 9](#_Toc496867031)

[10.3. Types of Users 10](#_Toc496867032)

[10.4. Network Architecture 11](#_Toc496867033)

[11. System Environment 11](#_Toc496867034)

[11.1. Hardware Inventory 12](#_Toc496867035)

[11.2. Software Inventory 12](#_Toc496867036)

[11.3. Network Inventory 12](#_Toc496867037)

[11.4. Data Flow 12](#_Toc496867038)

[11.5. Ports, Protocols, and Services 13](#_Toc496867039)

[12. System Interconnections 14](#_Toc496867040)

[13. FedRAMP Applicable Laws and Regulations 15](#_Toc496867041)

[13.1. FedRAMP Tailored LI-SaaS Guidance 15](#_Toc496867042)

[13.2. <*Information System Name*> APPLICABLE STANDARDS AND GUIDANCE 15](#_Toc496867043)

[14. Minimum Security Controls 16](#_Toc496867044)

[14.1. Access Control (AC) 24](#_Toc496867045)

[AC-2 Account Management 24](#_Toc496867046)

[AC-3 Access Enforcement 25](#_Toc496867047)

[AC-17 Remote Access 26](#_Toc496867048)

[AC-22 Publicly Accessible Content 27](#_Toc496867049)

[14.2. Audit and Accountability (AU) 29](#_Toc496867050)

[AU-3 Content of Audit Records 29](#_Toc496867051)

[AU-5 Response to Audit Processing Failure 30](#_Toc496867052)

[AU-6 Audit Review, Analysis, and Reporting 31](#_Toc496867053)

[14.3. Security Assessment and Authorization (CA) 33](#_Toc496867054)

[CA-2 Security Assessments 33](#_Toc496867055)

[CA-3 Internal System Connections (Conditional) 34](#_Toc496867056)

[CA-6 Security Authorization 36](#_Toc496867057)

[CA-7 Continuous Monitoring 37](#_Toc496867058)

[CA-9 Internal System Connections (Conditional) 40](#_Toc496867059)

[14.4. Configuration Management (CM) 41](#_Toc496867060)

[CM-4 Security Impact Analysis 41](#_Toc496867061)

[CM-6 Configuration Settings 42](#_Toc496867062)

[CM-8 Information System Component Inventory 44](#_Toc496867063)

[14.5. Contingency Planning (CP) 46](#_Toc496867064)

[CP-9 Information System Backup 46](#_Toc496867065)

[14.6. Identification and Authentication (IA) 47](#_Toc496867066)

[IA-2 (1) Identification and Authentication (Organization Users) | Network Access to Privileged Accounts 47](#_Toc496867067)

[IA-2 (12) Identification and Authentication (Organization Users) | Acceptance of PIV Credentials 49](#_Toc496867068)

[IA-5(11) Identification and Authentication (Organization Users) | Hardware Token-Based Authentication 50](#_Toc496867069)

[Control IA-6 Authenticator Feedback 51](#_Toc496867070)

[IA-8(1) Identification and Authentication (Non-Organization Users) | Acceptance of PIV Credentials from Other Agencies 52](#_Toc496867071)

[IA-8(2) Identification and Authentication (Non-Organization Users) | Acceptance of Third-Party Credentials 53](#_Toc496867072)

[14.7. Incident Response (IR) 54](#_Toc496867073)

[IR-4 Incident Handling 54](#_Toc496867074)

[IR-6 Incident Reporting 56](#_Toc496867075)

[14.8. Planning (PL) 57](#_Toc496867076)

[PL-2 System Security Plan 57](#_Toc496867077)

[14.9. Personnel Security (PS) 59](#_Toc496867078)

[PS-3 Personnel Screening 59](#_Toc496867079)

[14.10. Risk Assessment (RA) 61](#_Toc496867080)

[RA-2 Security Categorization 61](#_Toc496867081)

[RA-3 Risk Assessment 62](#_Toc496867082)

[RA-5 Vulnerability Scanning 64](#_Toc496867083)

[14.11. System and Services Acquisition (SA) 66](#_Toc496867084)

[SA-9 External Information System Services 66](#_Toc496867085)

[14.12. System and Communications Protection (SC) 68](#_Toc496867086)

[SC-5 Denial of Service Protection (Conditional) 68](#_Toc496867087)

[SC-7 Boundary Protection 69](#_Toc496867088)

[SC-12 Cryptographic Key Establishment & Management 70](#_Toc496867089)

[SC-13 Use of Cryptography 72](#_Toc496867090)

[14.13. System and Information Integrity (SI) 73](#_Toc496867091)

[SI-2 Flaw Remediation 73](#_Toc496867092)

[SI-3 Malicious Code Protection 74](#_Toc496867093)

[SI-4 Information System Monitoring 76](#_Toc496867094)

[15. Summary of Assessment Results 79](#_Toc496867095)

[16. Summary of Remediation Plans 81](#_Toc496867096)

[17. Acronyms 82](#_Toc496867097)

[18. ATTACHMENTS 83](#_Toc496867098)

[18.1. Recommended Attachment File Naming Convention 83](#_Toc496867099)

[18.2. ATTACHMENT 1 – FedRAMP *Tailored* LI-SaaS CIS Worksheet 83](#_Toc496867100)

[18.3. ATTACHMENT 2 – FedRAMP Inventory Workbook 83](#_Toc496867101)

[18.4. ATTACHMENT 3 – FedRAMP FIPS 199 Security Categorization 84](#_Toc496867102)

[18.5. ATTACHMENT 4 – <CSP/System Name> Summary of Remediation Plans 84](#_Toc496867103)

[18.6. ATTACHMENT 5 – FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Self-Attestation Requirements 84](#_Toc496867104)

[18.7. ATTACHMENT 6 – FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Continuous Monitoring Plan 84](#_Toc496867105)

List of Tables

[Table 1.1. Information System Identifier, Name, and Abbreviation 1](#_Toc496867183)

[Table 2.1. System Security Categorization 1](#_Toc496867184)

[Table 2.2. Information Type 2](#_Toc496867185)

[Table 2.3. Sensitivity Categorization of Information Types for the <Information System Abbreviation> 2](#_Toc496867186)

[Table 2.4. Security Impact Level 3](#_Toc496867187)

[Table 2.5. Baseline Security Configuration 3](#_Toc496867188)

[Table 3.1. Information System Owner 4](#_Toc496867189)

[Table 4.1. Independent Assessor 4](#_Toc496867190)

[Table 6.1. Information System AO Management Point of Contact 5](#_Toc496867191)

[Table 6.2. Information System AO Technical Point of Contact 5](#_Toc496867192)

[Table 7.1. Internal ISSO (or Equivalent) Point of Contact 6](#_Toc496867193)

[Table 7.2. AO ISSO Point of Contact 6](#_Toc496867194)

[Table 8.1. System Status 7](#_Toc496867195)

[Table 9.1. Determining a Cloud System 7](#_Toc496867196)

[Table 9.2. Service Layers Represented in this FedRAMP Tailored LI-SaaS Framework 8](#_Toc496867197)

[Table 9.3. Cloud Deployment Model Represented in this FedRAMP Tailored LI-SaaS Framework 8](#_Toc496867198)

[Table 9.4. Leveraged Authorizations 8](#_Toc496867199)

[Table 10.1. Personnel Roles and Privileges 10](#_Toc496867200)

[Table 11.1. Ports, Protocols, and Services 13](#_Toc496867201)

[Table 12.1. System Interconnections 14](#_Toc496867202)

[Table 13.1. FedRAMP Tailored LI-SaaS Applicable Guidance 15](#_Toc496867203)

[Table 13.2. <Information System Name> Standards and Guidance 15](#_Toc496867204)

[Table 14.1. Control Tailoring Criteria 16](#_Toc496867205)

[Table 14.2. Summary of FedRAMP Tailored LI-SaaS Security Controls 17](#_Toc496867206)

[Table 14.3. Control Origination and Definitions 23](#_Toc496867207)

[Table 14.4 Authorized Connections 35](#_Toc496867208)

[Table 15.1. Summary of Risks 79](#_Toc496867209)

[Table 15.2. <Independent Assessor Name> FedRAMP Tailored LI-SaaS CSP Team Members 79](#_Toc496867210)

[Table 15.3. <CSP Name> FedRAMP Tailored LI-SaaS CSP Team Members 80](#_Toc496867211)

[Table 18.1. Attachment File Naming Convention 83](#_Toc496867212)

List of Figures

[Figure 10.1. Authorization Boundary Diagram 9](#_Toc496867136)

[Figure 10.2. Network Diagram 11](#_Toc496867137)

[Figure 11.1. Data Flow Diagram 12](#_Toc496867138)

**FedRAMP *Tailored* LI-SaaS Framework Approvals**

Cloud Service Provider Signature

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name: | <Name> | | Date: | <Date> |
| Title: | <Title> | | | |
| Cloud Service Provider: | | <CSP Name> | | |
|  | | | | |
| Independent Assessor Signature | | | | |
|  | | | | |
| Name: | <Name> | | Date: | <Date> |
| Title: | <Title> | | | |
| Independent Assessor: | | <Assessor Name> | | |
|  | | | | |

# Information System Name

This FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Framework 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 (IT) systems is essential to ensure the required risk impact level of confidentiality, integrity, and availability of the data transmitted, processed, or stored by the *<Information System Abbreviation>* system is in place and operating as intended.

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

Table .1. Information System Identifier, Name, and Abbreviation

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

# Information System Categorization

The overall <*Information System Name*> sensitivity categorization is recorded in Table 2.1, Security Categorization, which follows. The completed FedRAMP FIPS 199 document is included in this document as Attachment 3 – FedRAMP FIPS Security Categorization.

Table 2.1. System Security Categorization

|  |  |
| --- | --- |
| **System Sensitivity Level:** | Low Impact |

## Information Types

This section describes how the information types used by the <*Information System Name*> are categorized for confidentiality, integrity, and availability of 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 the Office of Management and Budget (OMB) Federal Enterprise Architecture (EA) Program Management Office (PMO) Business Reference Model 2.0, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST Special Publication 800-60 (NIST SP 800-60) , *Guide for Mapping Types of Information and Information Systems to Security Categories*.

FIPS 199[[1]](#footnote-1) allows for a full range of information types. In order to meet specific, niche needs of systems, Agencies can specify the types of information being placed in the cloud environment. For FedRAMP *Tailored* LI-SaaS, Agencies can specify the type(s) of information that will reside in FedRAMP *Tailored* LI-SaaS applications/systems.

To be considered a FedRAMP *Tailored* LI-SaaS cloud application/service, the answer to all of the following questions must be “yes:”

1. Does the service operate in a cloud environment?
2. Is the cloud service fully operational?
3. Is the cloud service a Software as a Service (SaaS), as defined by NIST SP 800-145, The NIST Definition of Cloud Computing?
4. Does the cloud service contain no personally identifiable information (PII), except as needed to provide a login capability (username, password and email address)?
5. Is the cloud service low-security-impact, as defined by FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems?
6. Is the cloud service hosted within a FedRAMP-authorized Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), or is the CSP providing the underlying cloud infrastructure?

*Instruction: Record your information types in the tables that follow. 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:

Table .2. Information Type

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | Low | Low |

Table 2.3. Sensitivity Categorization of Information Types for the <Information System Abbreviation>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| *<Information Type>* | *<NIST Identifier>* | *Low* | *Low* | *Low* |
| *<Information Type>* | *<NIST Identifier>* | *Low* | *Low* | *Low* |
| *<Information Type>* | *<NIST Identifier>* | *Low* | *Low* | *Low* |

## Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2.3, Sensitivity Categorization of Information Types for the *<Information System Abbreviation>,* default to the high-water mark for the Information Types as identified in Table 2.4, Security Impact Level, below.

If the security impact level for confidentiality, integrity, and availability for any of the identified data types is moderate or high, the informationsystem is not a FedRAMP *Tailored* LI-SaaS system. The Cloud Service Provider (CSP) must meet the standard FedRAMP Low, Moderate, or High impact baseline security requirements, as applicable, and complete the requirement documentation.

Table 2.4. Security Impact Level

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

Through careful review and analysis, the baseline security categorization for the *<Information System Abbreviation>* system has been determined and is listed in Table 2.5, Baseline Security Configuration, which follows.

Table 2.5. Baseline Security Configuration

|  |  |
| --- | --- |
| ***<Information System Abbreviation>* Security Categorization** | Low |

Using this categorization, in conjunction with the risk assessment and any unique security requirements, the security controls for this system have been established as detailed in this FedRAMP *Tailored* LI-SaaS Framework.

# Information System Owner

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

Table 3.1. Information System Owner

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

# Independent Assessor

The following individual is identified as the Independent Assessor for this system.

Table 4.1. Independent Assessor

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

# Authorizing Official

The Authorizing Official (AO) or Designated Approving Authority (DAA) for the <*Information System Name*> is the <*Insert AO information>.*

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

Table 6.1. Information System AO Management Point of Contact

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

Table 6.2. Information System AO Technical Point of Contact

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

*Instruction: Add more tables as needed.*

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

# Assignment of Security Responsibility

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

Table 7.1. Internal ISSO (or Equivalent) Point of Contact

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

Table 7.2. AO ISSO Point of Contact

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

# Information System Operational Status

The system is currently in the life-cycle phase shown in Table 8.1, System Status, which follows. Only operational systems can be granted an Authority to Operate (ATO).

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

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

Table 8.1. System Status

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

# 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 can help system owners determine if their system is a cloud followed by specific questions to help system owners determine the type of cloud.

Table .1. Determining a Cloud System

|  |  |
| --- | --- |
| **Question (Yes/No)** | **Conclusion** |
| Does the system use virtual machines (VM)? | 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 customer to build anything other than servers? | A no response means that the system is an Infrastructure as a Service (IaaS). A yes response means that the system is either a Platform as a Service (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 Application Programming Interfaces (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 FedRAMP *Tailored* LI-SaaS Framework are indicated in Table 9.2, Service Layers Represented in this FedRAMP *Tailored* LI-SaaS Framework, which follows.

Table .2. Service Layers Represented in this FedRAMP Tailored LI-SaaS Framework

|  |  |  |
| --- | --- | --- |
| **Service Provider Architecture Layers** | | |
| ☐ | Software as a Service (SaaS) | Major Application |

## 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 FedRAMP Tailored LI-SaaS Framework, and that are not leveraged by any other FedRAMP Authorizations, are indicated in Table 9.3, Cloud Deployment Model Represented in this FedRAMP *Tailored* LI-SaaS Framework, which follows.

*Instruction: Check deployment model that applies.*

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

Table 9.3. Cloud Deployment Model Represented in this FedRAMP Tailored LI-SaaS Framework

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

## Leveraged Authorizations

The *<Information System Abbreviation>* leverages a pre-existing FedRAMP Authorized IaaS and/or PaaS. FedRAMP Authorizations leveraged by this *<Information System Abbreviation>* are listed in Table 9.4, Leveraged Authorizations, which follows.

Table 9.4. Leveraged Authorizations

|  |  |  |
| --- | --- | --- |
| **Leveraged Information System Name** | **Leveraged Service Provider Owner** | **Date Granted** |
| *<Leveraged information system name 1>* | *<Service provider owner 1>* | *<Date>* |
| *<Leveraged information system name 2>* | *<Service provider owner 2>* | *<Date>* |
| *<Leveraged information system name 3>* | *<Service provider owner 3>* | *<Date>* |

# General System Description

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

## 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 10.4), 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 10.1, Authorization Boundary Diagram, below.

|  |
| --- |
|  |

Figure .1. 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 10.1, Personnel Roles and Privileges, which 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 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 10.1. Personnel Roles and Privileges

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

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

## Network Architecture

*Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items, as applicable, 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, Virtual Local Area Networks (VLANs). Major security components should be represented. If necessary, include multiple network diagrams.*

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

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

The logical network topology is shown in Figure 10.2, Network Diagram, mapping the data flow between components.

Figure 10.2, Network Diagram(s), provides a visual depiction of the system network components that constitute the *<Information System Abbreviation>* system.

|  |
| --- |
|  |

Figure .2. 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.*

*The FedRAMP Inventory Workbook Template can be found on the FedRAMP website:* [*https://www.fedramp.gov/resources/templates-2016/*](https://www.fedramp.gov/resources/templates-2016/)

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

The FedRAMP Inventory Workbook is included in this document in ATTACHMENT 2 – FedRAMP Inventory Workbook.

## 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.*

*Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users.*

*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 11.1, Data Flow Diagram, below.

|  |
| --- |
|  |

Figure .1. Data Flow Diagram

## Ports, Protocols, and Services

Table 11.1, Ports, Protocols, and Services, lists the ports, protocols, and services enabled for the <*Information System Abbreviation>.*

*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 as applicable for this application/service and as applicable for the leveraged system. Add more rows as needed.*

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

Table 11.1. Ports, Protocols, and Services

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

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

Table 12.1, System Interconnections, is consistent with the CA-3 Authorized Connections attestation information.

Table 12.1. System Interconnections

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

# FedRAMP Applicable Laws and Regulations

The FedRAMP Laws and Regulations Template can be found on this page: <https://www.fedramp.gov/resources/templates-2016/>.

## FedRAMP Tailored LI-SaaS Guidance

Table 13.1, FedRAMP *Tailored* LI-SaaS Applicable Guidance, includes additional documentation specific to FedRAMP *Tailored* LI-SaaS information systems.

Table .1. FedRAMP Tailored LI-SaaS Applicable Guidance

|  |  |
| --- | --- |
| **Title** | **Date** |
| FedRAMP *Tailored* Security Requirements for Low Impact Software as a Service (LI-SaaS) Cloud Systems | 1/30/2017 |
| NIST SP 800-171 rev 1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations | 12/2016 |
| NIST Framework for Improving Critical Infrastructure Cybersecurity, v1.0 | 2/12/2014 |

.

## <*Information System Name*> APPLICABLE STANDARDS AND GUIDANCE

Table 13.2, <*Information System Name>* Standards and Guidance, includes any additional standards and guidance specific to <*Information System Name*>.

Table .2. <Information System Name> Standards and Guidance

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

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. The following table contains the FedRAMP *Tailored* LI-SaaS minimum baseline controls (by family) that have been carved out from the security controls in the FedRAMP LI Security Baseline in accordance with the tailoring criteria established by NIST and FedRAMP.

There are six (6) categories of FedRAMP *Tailored* LI-SaaS controls: FED, NSO, Required, Conditional, Inherited, and Attestation. Table 14.1, Control Tailoring Criteria, provides definitions of the tailoring criteria utilized for the determination of the FedRAMP *Tailored* LI-SaaS baseline.

Table .1. Control Tailoring Criteria

| **Tailoring Symbol** | **Tailoring Criteria** | **CSP Response Requirements** |
| --- | --- | --- |
| FED | Controls that are uniquely Federal, which are primarily the responsibility of the Federal Government. | No CSP response is required. |
| NSO | Controls FedRAMP determined not to have an impact on the security of the FedRAMP *Tailored* LI-SaaS. | No CSP response is required. |
| Required | Controls FedRAMP determined to be required for the FedRAMP *Tailored* LI-SaaS. | CSP response to control requirements is required. |
| Conditional | Controls FedRAMP determined to be conditionally required for the FedRAMP *Tailored* LI-SaaS. | CSP response to control requirements is required. |
| Inherited | Controls FedRAMP determined to be inherited from the underlying infrastructure provider (i.e., FedRAMP authorized IaaS/PaaS). | CSP attestation response is required. |
| Attestation | Controls FedRAMP determined that the CSP is required to attest to being in place and operating as intended for the FedRAMP *Tailored* LI-SaaS. | CSP attestation response is required. |

The CSP response for all controls requiring an attestation of the status and implementation of the security requirements is defined in the FedRAMP *Tailored* LI-SaaS CSP Self-Attestation table. (See Attachment 5, FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Self-Attestation Requirements).

Table 14.2, Summary of FedRAMP *Tailored* LI-SaaS Security Controls, lists all the controls required for the FedRAMP Low Impact Baseline and the associated tailoring criteria for each control.

Table .2. Summary of FedRAMP Tailored LI-SaaS Security Controls

| **ID** | **Control Description** | **FedRAMP *Tailored* LI-SaaS Controls** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **FED** | **NSO** | **Required** | **Conditional** | **Inherited** | **Attestation Required** |
| **AC – Access Control** | | | | | | | |
| **AC-1** | Access Control Policy and Procedures |  |  |  |  |  | X |
| **AC-2** | Account Management |  |  | x |  |  |  |
| **AC-3** | Access Enforcement |  |  | x |  |  |  |
| **AC-7[[2]](#footnote-2)** | Unsuccessful Logon Attempts |  | x |  |  |  | x |
| **AC-8** | System Use Notification | x |  |  |  |  |  |
| **AC-14** | Permitted Actions without Identification or Authentication | x |  |  |  |  |  |
| **AC-17** | Remote Access |  |  | x |  |  |  |
| **AC-18** | Wireless Access |  | x |  |  |  |  |
| **AC-19** | Access Control for Mobile Devices |  | x |  |  |  |  |
| **AC-20** | Use of External Information Systems |  |  |  |  |  | x |
| **AC-22** | Publicly Accessible Content |  |  | x |  |  |  |
| **AT – Awareness and Training** | | | | | | | |
| **AT-1** | Security Awareness and Training Policy and Procedures |  |  |  |  |  | x |
| **AT-2** | Security Awareness Training |  |  |  |  |  | x |
| **AT-3** | Role-Based Security Training |  |  |  |  |  | x |
| **AT-4** | Security Training Records |  |  |  |  |  | x |
| **AU – Audit and Accountability** | | | | | | | |
| **AU-1** | Audit and Accountability Policy and Procedures |  |  |  |  |  | x |
| **AU-2** | Audit Events |  |  |  |  |  | x |
| **AU-3** | Content of Audit Records |  |  | x |  |  |  |
| **AU-4** | Audit Storage Capacity |  | x |  |  |  |  |
| **AU-5** | Response to Audit Processing Failures |  |  | x |  |  |  |
| **AU-6** | Audit Review, Analysis, and Reporting |  |  | x |  |  |  |
| **AU-8** | Time Stamps |  |  |  |  |  | x |
| **AU-9** | Protection of Audit Information |  |  |  |  |  | x |
| **AU-11** | Audit Record Retention |  | x |  |  |  |  |
| **AU-12** | Audit Generation |  |  |  |  |  | x |
| **CA – Security Assessment and Authorization** | | | | | | | |
| **CA-1** | Security Assessment and Authorization Policies and Procedures |  |  |  |  |  | x |
| **CA-2** | Security Assessments |  |  | x |  |  |  |
| **CA-2(1)** | Security Assessments | Independent Assessors |  |  |  |  |  | x |
| **CA-3** | System Interconnections |  |  | x | x |  |  |
| **CA-5[[3]](#footnote-3)** | Plan of Action and Milestones |  |  |  |  |  | x |
| **CA-6** | Security Authorization |  |  | x |  |  |  |
| **CA-7** | Continuous Monitoring |  |  | x |  |  |  |
| **CA-9[[4]](#footnote-4)** | Internal System Connections |  |  | x | x |  |  |
| **CM – Configuration Management** | | | | | | | |
| **CM-1** | Configuration Management Policy and Procedures |  |  |  |  |  | x |
| **CM-2** | Baseline Configuration |  |  |  |  |  | x |
| **CM-4** | Security Impact Analysis |  |  | x |  |  |  |
| **CM-6[[5]](#footnote-5)** | Configuration Settings |  |  | x |  |  |  |
| **CM-7** | Least Functionality |  |  |  |  |  | x |
| **CM-8** | Information System Component Inventory |  |  | x |  |  |  |
| **CM-10** | Software Usage Restrictions |  | x |  |  |  |  |
| **CM-11** | User Installed Software |  | x |  |  |  |  |
| **CP – Contingency Planning** | | | | | | | |
| **CP-1** | Contingency Planning Policy and Procedures |  |  |  |  |  | x |
| **CP-2** | Contingency Plan |  | x |  |  |  |  |
| **CP-3** | Contingency Training |  | x |  |  |  |  |
| **CP-4** | Contingency Plan Testing |  | x |  |  |  |  |
| **CP-9** | Information System Backup |  |  | x |  |  |  |
| **CP-10** | Information System Recovery and Reconstitution |  | x |  |  |  |  |
| **IA – Identification and Authentication** | | | | | | | |
| **IA-1** | Identification and Authentication Policy and Procedures |  |  |  |  |  | x |
| **IA-2[[6]](#footnote-6)** | Identification and Authentication (Organizational Users) |  | x |  |  |  | x |
| **IA-2 (1)** | Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts |  |  | x |  |  |  |
| **IA-2(12)[[7]](#footnote-7)** | Identification and Authentication  (Organizational Users) | Acceptance of PIV Credentials |  |  | x | x |  |  |
| **IA-4** | Identifier Management |  |  |  |  |  | x |
| **IA-5** | Authenticator Management |  |  |  |  |  | x |
| **IA-5 (1)** | Authenticator Management | Password-Based Authentication |  |  |  |  |  | x |
| **IA-5(11)[[8]](#footnote-8)** | Authenticator Management | Hardware Token-Based Authentication | x |  | x | x |  |  |
| **IA-6** | Authenticator Feedback |  |  | x |  |  |  |
| **IA-7** | Cryptographic Module Authentication |  |  |  |  |  | x |
| **IA-8** | Identification and Authentication (Non-Organizational Users) |  |  |  |  |  | x |
| **IA-8(1)[[9]](#footnote-9)** | Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies |  |  | x | x |  |  |
| **IA-8(2)[[10]](#footnote-10)** | Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials |  |  | x | x |  |  |
| **IA-8(3)** | Identification and Authentication (Non-Organizational Users) | Acceptance of FICAM-Approved Products |  |  |  |  |  | x |
| **IA-8(4)** | Identification and Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles |  |  |  |  |  | x |
| **IR – Incident Response** | | | | | | | |
| **IR-1** | Incident Response Policy and Procedures |  |  |  |  |  | x |
| **IR-2** | Incident Response Training |  |  |  |  |  | x |
| **IR-4** | Incident Handling |  |  | x |  |  |  |
| **IR-5** | Incident Monitoring |  |  |  |  |  | x |
| **IR-6** | Incident Reporting |  |  | x |  |  |  |
| **IR-7** | Incident Response Assistance |  |  |  |  |  | x |
| **IR-8[[11]](#footnote-11)** | Incident Response Plan |  |  |  |  |  | x |
| **IR-9[[12]](#footnote-12)** | Information Spillage Response |  |  |  |  |  | x |
| **MA – Maintenance [[13]](#footnote-13)** | | | | | | | |
| **MA-1** | System Maintenance Policy and Procedures |  |  |  |  |  | x |
| **MA-2** | Controlled Maintenance |  |  | x |  | x | x |
| **MA-4** | Nonlocal Maintenance |  |  |  |  |  | x |
| **MA-5** | Maintenance Personnel |  |  | x |  | x | x |
| **MP – Media Protection[[14]](#footnote-14)** | | | | | | | |
| **MP-1** | Media Protection Policy and Procedures |  |  |  |  |  | x |
| **MP-2** | Media Access |  |  | x |  | x | x |
| **MP-6** | Media Sanitization |  |  | x |  | x | x |
| **MP-7** | Media Use |  |  | x |  | x | x |
| **PE – Physical and Environmental Protection[[15]](#footnote-15)** | | | | | | | |
| **PE-1** | Physical and Environmental Protection Policy and Procedures |  |  |  |  |  | x |
| **PE-2** | Physical Access Authorizations |  |  | x |  | x | x |
| **PE-3** | Physical Access Control |  |  | x |  | x | x |
| **PE-6** | Monitoring Physical Access |  |  | x |  | x | x |
| **PE-8** | Visitor Access Records |  |  | x |  | x | x |
| **PE-12** | Emergency Lighting |  |  | x |  | x | x |
| **PE-13** | Fire Protection |  |  | x |  | x | x |
| **PE-14** | Temperature and Humidity Controls |  |  | x |  | x | x |
| **PE-15** | Water Damage Protection |  |  | x |  | x | x |
| **PE-16** | Delivery and Removal |  |  | x |  | x | x |
| **PL – Planning** | | | | | | | |
| **PL-1** | Security Planning Policy and Procedures |  |  |  |  |  | x |
| **PL-2** | System Security Plan |  |  | x |  |  |  |
| **PL-4** | Rules of Behavior |  |  |  |  |  | x |
| **PS – Personnel Security** | | | | | | | |
| **PS-1** | Personnel Security Policy and Procedures |  |  |  |  |  | x |
| **PS-2** | Position Risk Designation | x |  |  |  |  |  |
| **PS-3** | Personnel Screening |  |  | x |  |  |  |
| **PS-4** | Personnel Termination |  |  |  |  |  | x |
| **PS-5** | Personnel Transfer |  |  |  |  |  | x |
| **PS-6** | Access Agreements |  |  |  |  |  | x |
| **PS-7** | Third-Party Personnel Security |  |  |  |  |  | x |
| **PS-8** | Personnel Sanctions |  |  |  |  |  | x |
| **RA – Risk Assessment** | | | | | | | |
| **RA-1** | Risk Assessment Policy and Procedures |  |  |  |  |  | x |
| **RA-2** | Security Categorization |  |  | x |  |  |  |
| **RA-3** | Risk Assessment |  |  | x |  |  |  |
| **RA-5** | Vulnerability Scanning |  |  | x |  |  |  |
| **SA – System and Services Acquisition** | | | | | | | |
| **SA-1** | System and Services Acquisition Policy and Procedures |  |  |  |  |  | x |
| **SA-2** | Allocation of Resources |  |  |  |  |  | x |
| **SA-3** | System Development Life Cycle |  |  |  |  |  | x |
| **SA-4** | Acquisition Process |  |  |  |  |  | x |
| **SA-4(10)** | Acquisition Process | Use of Approved PIV |  |  |  |  |  | x |
| **SA-5** | Information System Documentation |  |  |  |  |  | x |
| **SA-9** | External Information System Services |  |  | x |  |  |  |
| **SC – System and Communications Protection** | | | | | | | |
| **SC-1** | System and Communications Protection Policy and Procedures |  |  |  |  |  | x |
| **SC-5[[16]](#footnote-16)** | Denial of Service Protection |  |  | x | x |  |  |
| **SC-7** | Boundary Protection |  |  | x |  |  |  |
| **SC-12** | Cryptographic Key Establishment and Management |  |  | x |  |  |  |
| **SC-13[[17]](#footnote-17)** | Cryptographic Protection |  |  | x | x |  |  |
| **SC-15** | Collaborative Computing Devices |  | x |  |  |  |  |
| **SC-20** | Secure Name /Address Resolution Service (Authoritative Source) |  |  |  |  |  | x |
| **SC-21** | Secure Name /Address Resolution Service (Recursive or Caching Resolver) |  |  |  |  |  | x |
| **SC-22** | Architecture and Provisioning for  Name/Address Resolution Service |  |  |  |  |  | x |
| **SC-39** | Process Isolation |  |  |  |  |  | x |
| **SI – System and Information Integrity** | | | | | | | |
| **SI-1** | System and Information Integrity Policy and Procedures |  |  |  |  |  | x |
| **SI-2** | Flaw Remediation |  |  | x |  |  |  |
| **SI-3** | Malicious Code Protection |  |  | x |  |  |  |
| **SI-4** | Information System Monitoring |  |  | x |  |  |  |
| **SI-5** | Security Alerts, Advisories, and Directives |  |  |  |  |  | x |
| **SI-12[[18]](#footnote-18)** | Information Handling and Retention |  |  |  |  |  | x |

*Instruction: In the sections that follow, fully describe how the information security control is implemented in 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 FedRAMP* Tailored *LI-SaaS Framework, if documentation is referenced (e.g., policies and procedures), they 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.*

*If there are additional CSP-specific inherited control requirements that are partially or fully inherited from the IaaS or PaaS, the “inherited” check box must be checked and the implementation description must simply describe “what is inherited.”*

*If the CSP is providing the underlying cloud infrastructure, some controls become required rather than attested to. They are noted in the above table and Appendix A – FedRAMP Tailored Security Controls Baseline. The AO is encouraged to consider evidence from other compliance regimes as an approach to validating control implementation.*

*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.*

*The information in each of the FedRAMP* Tailored *LI-SaaS Framework components must be provided in sufficient detail about the service itself, and its associated risk posture, to support Federal entities in making risk-based decisions for issuing ATOs.*

* *Responsible Role – Indicates the role of CSP employee(s) responsible for implementing the control*.
* *Control Implementation – Descriptions of control implementations must provide sufficient detail that the implementation can be validated/assessed. This includes descriptions of what and how the security controls are implemented by the CSP. For example, some controls are fully implemented by the CSP and some controls have a “shared” implementation with either the underlying PaaS/IaaS and/or the customer user. Clear and concise descriptions of what is being provided by the “shared” entity must be included.*
* *Assessment Plan/Procedures – Descriptions of the procedures for validating and assessing the security control implementations must be provided. If the assessor intends to incorporate assessments conducted by other entities as validation of the control, details of those assessments and determination of specific applicability must be provided.*
* *Assessment Results – Descriptions of the results of the validation/assessment must be provided, including whether the required control is fully implemented or other than fully implemented. For requirements that are not fully implemented, there must be a complete description of the weakness identified, including the risk level impact to the security posture of the system (High, Moderate, or Low). Information about documentation/ observations/interviews and evidence collected must be provided in support of the implementation status determination.*
* *Remediation Plan – Descriptions of the plan for remediating and/or mitigating the validation/assessment risks identified must be described.*

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

The definitions in Table 14.3, Control Origination and Definitions, indicate where each security control originates.

Table .3. Control Origination and Definitions

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| 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 Security Assertions Markup Language (SAML) Single Sign-On (SSO) solution to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the CSP Name and partially by the customer. | Security awareness training must be conducted by both the CSPN and the customer. |
| Inherited from pre-existing FedRAMP Authorization | A control that is inherited from another CSP Name system that has already received a FedRAMP Authorization. | A PaaS or SaaS provider inherits Physical and Environmental (PE) controls from an IaaS provider. |

## Access Control (AC)

### AC-2 Account Management

|  |
| --- |
| **AC-2 Requirement(s)** |
| 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. [Excluded from FedRAMP Tailored for LI-SaaS] 3. [Excluded from FedRAMP Tailored for LI-SaaS] 4. [Excluded from FedRAMP Tailored for LI-SaaS] 5. [Excluded from FedRAMP Tailored for LI-SaaS] 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; and 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. [Excluded from FedRAMP Tailored for LI-SaaS] 10. [Excluded from FedRAMP Tailored for LI-SaaS] 11. [Excluded from FedRAMP Tailored for LI-SaaS] |
| **AC-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **AC-2 What is the solution and how is it implemented?** |
| Description of how AC-2 is implemented,  Customer Responsibilities |
| **AC-2 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization defines information system account types to be identified and selected to support organizational missions/business functions.  **Assessment Procedures**   * **Examine:** Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of active system accounts along with the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; information system monitoring records; information system audit records; other relevant documents or records. * **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. * **Test:** Organizational processes for account management on the information system; automated mechanisms for implementing account management. |
| **AC-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **AC-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### AC-3 Access Enforcement

|  |
| --- |
| **AC-3 Requirement(s)** |
| The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. |
| **AC-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **AC-3 What is the solution and how is it implemented?** |
| Description of how AC-3 is implemented.  Customer Responsibilities |
| **AC-3 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.  **Assessment Procedures**   * Examine - Access control policy; procedures addressing access enforcement; information system design documentation; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; and other relevant documents or records. * Interview - Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; and system developers. * Test - Automated mechanisms implementing access control policy. |
| **AC-3 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **AC-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### AC-17 Remote Access

|  |
| --- |
| **AC-17 Requirement(s)** |
| The organization:   1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and 2. Authorizes remote access to the information system prior to allowing such connections. |
| **AC-17 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **AC-17 What is the solution and how is it implemented?** |
| Description of how AC-17 is implemented.  Customer Responsibilities |
| **AC-17 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization authorizes remote access to the information system prior to allowing such connections  **Assessment Procedures**   * Examine - Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; security plan; information system configuration settings and associated documentation; remote access authorizations; information system audit records; and other relevant documents or records. * Interview - Organizational personnel with responsibilities for managing remote access connections; system/network administrators; and organizational personnel with information security responsibilities. * Test - Remote access management capability for the information system. |
| **AC-17 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **AC-17 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### AC-22 Publicly Accessible Content

|  |
| --- |
| **AC-22 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| A**C-22 What is the solution and how is it implemented?** |
| Description of how AC-22 is implemented.  Customer Responsibilities |
| **AC-22 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization designates individuals authorized to post information onto a publicly accessible information system.  **Assessment Procedures**   * Examine - Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records Interview - Organizational personnel with responsibilities for managing remote access connections; system/network administrators; and organizational personnel with information security responsibilities. * Interview - Organizational personnel with responsibilities for managing publicly accessible information posted on organizational information systems; and organizational personnel with information security responsibilities. * Test - Automated mechanisms implementing management of publicly accessible content. |
| **AC-22 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **AC-22 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Audit and Accountability (AU)

### AU-3 Content of Audit Records

|  |
| --- |
| **AU-3 Requirement(s)** |
| The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. |
| **AU-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **AU-3 What is the solution and how is it implemented?** |
| Description of how AU-3 is implemented.  Customer Responsibilities |
| **AU-3 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if 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   + The identity of any individuals or subjects associated with the event   **Assessment Procedures**   * Examine - Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; information system incident reports; and other relevant documents or records. * Interview - Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; and system/network administrators. * Test - Automated mechanisms implementing information system auditing of auditable events. |
| **AU-3 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system. |
| **AU-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### AU-5 Response to Audit Processing Failure

|  |
| --- |
| **AU-5 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **AU-5 What is the solution and how is it implemented?** |
| Description of how AU-5 is implemented.  Customer Responsibilities |
| **AU-5 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization defines the personnel or roles to be alerted in the event of an audit processing failure.  **Assessment Procedures**   * Examine - Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; and other relevant documents or records. * Interview - Organizational personnel with responsibilities for managing remote access connections; system/network administrators; and organizational personnel with information security responsibilities. * Interview - Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; and system/network administrators; system developers. * Test - Automated mechanisms implementing information system response to audit processing failures. |
| **AU-5 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system. |
| **AU-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

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

|  |
| --- |
| **AU-6 Requirement(s)** |
| The organization:   1. Reviews and analyzes information system audit records [*FedRAMP Assignment: at least weekly*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and 2. Reports findings to [*Assignment: organization-defined personnel or roles*]. |
| **AU-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **AU-6 What is the solution and how is it implemented?** |
| Description of how AU-6 is implemented.  Customer Responsibilities |
| **AU-6 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization   * Defines the types of inappropriate or unusual activity to look for when information system audit records are reviewed and analyzed. * Defines the frequency to review and analyze information system audit records for indications of organization-defined inappropriate or unusual activity. * Reviews and analyzes information system audit records for indications of organization-defined inappropriate or unusual activity with the organization-defined frequency. * Defines personnel or roles to whom findings resulting from reviews and analysis of information system audit records are to be reported. * Reports findings to organization-defined personnel or roles.   **Assessment Procedures**   * Examine - Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; and other relevant documents or records. * Interview - Organizational personnel with audit review, analysis, and reporting responsibilities; and organizational personnel with information security responsibilities. * Test - N/A |
| **AU-6 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system. |
| **AU-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Security Assessment and Authorization (CA)

### CA-2 Security Assessments

|  |
| --- |
| **CA-2 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CA-2 What is the solution and how is it implemented?** |
| Description of how CA-2 is implemented.  Customer Responsibilities |
| **CA-2 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Develops a security assessment plan that describes the scope of the assessment including:   + Security controls and control enhancements under assessment.   + Assessment procedures to be used to determine security control effectiveness.   + Assessment environment.   + Assessment team.     - Assessment roles and responsibilities. * Defines the frequency to assess the security controls in the information system and its environment of operation * Assesses the security controls in the information system with the organization-defined frequency 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. * Produces a security assessment report that documents the results of the assessment. * Defines individuals or roles to whom the results of the security control assessment are to be provided. * Provides the results of the security control assessment to organization-defined individuals or roles.   **Assessment Procedures**   * Examine - Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; and other relevant documents or records. * Interview - Organizational personnel with security assessment responsibilities; and organizational personnel with information security responsibilities. * Test - Automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting. |
| **CA-2 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **CA-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### CA-3 Internal System Connections (Conditional)

|  |
| --- |
| **CA-3 Requirement(s)** |
| 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*]. |
| **CA-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| C**A-3 What is the solution and how is it implemented?** |
| Description of how CA-3 is implemented.  Customer Responsibilities  **Complete *Table 13-3 CA-3 Authorized Connections*, below.** |
| **CA-3 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements. * Documents, for each interconnection:   + The interface characteristics;   + The security requirements; and   + The nature of the information communicated. * Defines the frequency to review and update Interconnection Security Agreements. * Reviews and updates Interconnection Security Agreements with the organization-defined frequency   **Assessment Procedures**   * Examine - Access control policy; procedures addressing information system connections; system and communications protection policy; security plan; information system design documentation; information system configuration settings and associated documentation; list of components or classes of components authorized as system interconnections; security assessment report; information system audit records; and other relevant documents or records. * Interview -Organizational personnel with responsibility for developing, implementing, or authorizing system interconnections; organizational personnel with information security responsibilities. * Test - N/A |
| **CA-3 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **CA-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

Table .4 Authorized Connections

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

### CA-6 Security Authorization

|  |
| --- |
| **CA-6 Requirement(s)** |
| The organization:   1. Assigns a senior-level executive or manager as the authorizing official for the information system; 2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and 3. Updates the security authorization [*FedRAMP Assignment: at least every three years or when a significant change occurs*].   **CA-6c Additional FedRAMP Requirements and Guidance:** Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the Authorizing Official. |
| **CA-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CA-6 What is the solution and how is it implemented?** |
| Description of how CA-6 is implemented.  Customer Responsibilities |
| **CA-6 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization**:**   * Assigns a senior-level executive or manager as the authorizing official for the information system. * Ensures that the authorizing official authorizes the information system for processing before commencing operations. * Defines the frequency to update the security authorization. * Updates the security authorization with the organization-defined frequency.   **Assessment Procedures**   * Examine -Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); and other relevant documents or records. * Interview - Organizational personnel with security authorization responsibilities; and organizational personnel with information security responsibilities. * Test - Automated mechanisms that facilitate security authorizations and updates. |
| **CA-6 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **CA-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### CA-7 Continuous Monitoring

|  |
| --- |
| **CA-7 Requirement(s)** |
| The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:   1. Establishment of [*Assignment: organization-defined metrics*] to be monitored; 2. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring; 3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; 4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; 5. Correlation and analysis of security-related information generated by assessments and monitoring; 6. Response actions to address results of the analysis of security-related information; and 7. Reporting the security status of organization and the information system to [*FedRAMP Assignment: to meet Federal and FedRAMP requirements*] [*Assignment: organization-defined frequency*].   **CA-7 Additional FedRAMP Requirements and Guidance:** CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates. |
| **CA-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CA-7 What is the solution and how is it implemented?** |
| Description of how CA-7 is implemented.  Customer Responsibilities |
| **CA-7 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Develops a continuous monitoring strategy that defines metrics to be monitored. * Develops a continuous monitoring strategy that includes monitoring of organization-defined metrics. * Implements a continuous monitoring program that includes monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy. * Develops a continuous monitoring strategy that defines frequencies for monitoring and defines frequencies for assessments supporting monitoring. * Develops a continuous monitoring strategy that includes establishment of the organization-defined frequencies for monitoring and for assessments supporting monitoring. * Implements a continuous monitoring program that includes establishment of organization-defined frequencies for monitoring and for assessments supporting such monitoring in accordance with the organizational continuous monitoring strategy. * Develops a continuous monitoring strategy that includes ongoing security control assessments. * Implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy. * Develops a continuous monitoring strategy that includes ongoing security status monitoring of organization-defined metrics. * Implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy. * Develops a continuous monitoring strategy that includes correlation and analysis of security-related information generated by assessments and monitoring. * Implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring in accordance with the organizational continuous monitoring strategy. * Develops a continuous monitoring strategy that includes response actions to address results of the analysis of security-related information. * Implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information in accordance with the organizational continuous monitoring strategy. * Develops a continuous monitoring strategy that defines the personnel or roles to whom the security status of the organization and information system are to be reported. * Develops a continuous monitoring strategy that defines the frequency to report the security status of the organization and information system to organization-defined personnel or roles. * Develops a continuous monitoring strategy that includes reporting the security status of the organization or information system to organizational-defined personnel or roles with the organization-defined frequency. * Implements a continuous monitoring program that includes reporting the security status of the organization and information system to organization-defined personnel or roles with the organization-defined frequency in accordance with the organizational continuous monitoring strategy.     **Assessment Procedures**   * Examine -Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; and other relevant documents or records. * Interview –Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security responsibilities; and system/network administrators. * Test – Mechanisms implementing continuous monitoring. |
| **CA-7 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **CA-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### CA-9 Internal System Connections (Conditional)

|  |
| --- |
| **CA-9 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| C**A-9 What is the solution and how is it implemented?** |
| Description of how CA-9 is implemented.  Customer Responsibilities |
| **CA-9 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines information system components or classes of components to be authorized as internal connections to the information system. * Authorizes internal connections of organization-defined information system components or classes of components to the information system. * Documents, for each internal connection:   + The interface characteristics;   + The security requirements; and   + The nature of the information communicated.   **Assessment Procedures**   * Examine - Access control policy; procedures addressing information system connections; system and communications protection policy; security plan; information system design documentation; information system configuration settings and associated documentation; list of components or classes of components authorized as internal system connections; security assessment report; information system audit records; and other relevant documents or records. * Interview - **9.a.2 only:** Organizational personnel with responsibility for developing, implementing, or authorizing internal system connections; organizational personnel with information security responsibilities. * Test - N/A |
| **CA-9 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **CA-9 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Configuration Management (CM)

### CM-4 Security Impact Analysis

|  |
| --- |
| **CM-4 Requirement(s)** |
| The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. |
| **CM-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CM-4 What is the solution and how is it implemented?** |
| Description of how CM-4 is implemented.  Customer Responsibilities |
| **CM-4 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.  **Assessment Procedures**   * Examine - Configuration management policy; procedures addressing security impact analysis for changes to the information system; configuration management plan; security impact analysis documentation; analysis tools and associated outputs; change control records; information system audit records; and other relevant documents or records. * Interview - Organizational personnel with responsibility for conducting security impact analysis; organizational personnel with information security responsibilities; and system/network administrators. * Test - Organizational processes for security impact analysis. |
| **CM-4 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system |
| **CM-4 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### CM-6 Configuration Settings

|  |
| --- |
| **CM-6 Requirement(s)** |
| The organization:   1. Establishes and documents configuration settings for information technology products employed within the information system using [*FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance*] that reflect the most restrictive mode consistent with operational requirements;   **CM-6(a) Additional FedRAMP Requirements and Guidance:**  **Requirement 1:** The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available.  **Requirement 2:** The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).  **Guidance:** Information on the USGCB checklists can be found at: <http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc>   1. Implements the configuration settings; 2. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and 3. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.   **Note:** Information on the USGCB checklists can be found at: [*http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc\*](http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc/)  Information on SCAP can be found at: [*http://scap.nist.gov/*](http://scap.nist.gov/) |
| **CM-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CM-6 What is the solution and how is it implemented?** |
| Description of how CM-6 is implemented.  Customer Responsibilities |
| **CM-6 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines security configuration checklists to be used to establish and document configuration settings for the information technology products employed. * Ensures the defined security configuration checklists reflect the most restrictive mode consistent with operational requirements. * Establishes and documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists. * Implements the configuration settings established/documented in CM-6(a). * Defines information system components for which any deviations from established configuration settings must be: * Identified; * Documented; and * Approved. * Defines operational requirements to support: * The identification of any deviations from established configuration settings; * The documentation of any deviations from established configuration settings; and * The approval of any deviations from established configuration settings. * Identifies any deviations from established configuration settings for organization-defined information system components based on organizational-defined operational requirements. * Approves any deviations from established configuration settings for organization-defined information system components based on organizational-defined operational requirements. * Monitors changes to the configuration settings in accordance with organizational policies and procedures. * Controls changes to the configuration settings in accordance with organizational policies and procedures.   **Assessment Procedures**   * Examine - Configuration management policy; procedures addressing configuration settings for the information system; configuration management plan; security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; evidence supporting approved deviations from established configuration settings; change control records; information system audit records; and other relevant documents or records. * Interview - Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; and system/network administrators. * Test - Organizational processes for managing configuration settings; automated mechanisms that implement, monitor, and/or control information system configuration settings; and automated mechanisms that identify and/or document deviations from established configuration settings. |
| **CM-6 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented – description of weakness and risk to the system. |
| **CM-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### CM-8 Information System Component Inventory

|  |
| --- |
| **CM-8 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CM-8 What is the solution and how is it implemented?** |
| Description of how CM-8 is implemented.  Customer Responsibilities |
| **CM-8 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Develops and documents an inventory of information system components that accurately reflects the current information system. * Develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system. * Develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting. * Defines the information deemed necessary to achieve effective information system component accountability. * Develops and documents an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability. * Defines the frequency to review and update the information system component inventory. * Reviews and updates the information system component inventory with the organization-defined frequency.   **Assessment Procedures**   * Examine - Configuration management policy; procedures addressing information system component inventory; configuration management plan; security plan; information system inventory records; inventory reviews and update records; and other relevant documents or records. * Interview - Organizational personnel with responsibilities for information system component inventory; organizational personnel with information security responsibilities; and system/network administrators. * Test - Organizational processes for developing and documenting an inventory of information system components; automated mechanisms supporting and/or implementing the information system component inventory. |
| **CM-8 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **CM-8 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Contingency Planning (CP)

### CP-9 Information System Backup

|  |
| --- |
| **CP-9 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **CP-9 What is the solution and how is it implemented?** |
| Description of how CP-9 is implemented.  Customer Responsibilities |
| **CP-9 Assessment Plan/Procedures** |
| **Assessment Objectives**  Determine if the organization:   * Defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system. * Conducts backups of user-level information contained in the information system with the organization-defined frequency. * Defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of system-level information contained in the information system. * Conducts backups of system-level information contained in the information system with the organization-defined frequency. * Defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of information system documentation including security-related documentation. * Conducts backups of information system documentation, including security-related documentation, with the organization-defined frequency. * Protects the confidentiality, integrity, and availability of backup information at storage locations.   **Assessment Procedures**   * Examine - Contingency planning policy; procedures addressing information system backup; contingency plan; backup storage location(s);information system backup logs or records; and other relevant documents or records. * Interview - Organizational personnel with information system backup responsibilities; and organizational personnel with information security responsibilities. * Test - Organizational processes for conducting information system backups; automated mechanisms supporting and/or implementing information system backups. |
| **CP-9 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented.  If other than implemented, description of weakness and risk to the system. |
| **CP-9 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Identification and Authentication (IA)

### IA-2 (1) Identification and Authentication (Organization Users) | Network Access to Privileged Accounts

|  |
| --- |
| **IA-2 (1) Requirement(s)** |
| The information system implements multifactor authentication for network access to privileged accounts. |
| **IA-2 (1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IA-2 (1) What is the solution and how is it implemented?** |
| Description of how IA-2 (1) is implemented.  Customer Responsibilities |
| **IA-2 (1) Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization implements multifactor authentication for network access to privileged accounts.  **Assessment Procedures**   * Examine - Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; and other relevant documents or records. * Interview - Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; and system/network administrators; system developer. * Test - Automated mechanisms supporting and/or implementing multifactor authentication capability. |
| **IA-2 (1) Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IA-2(2)Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### IA-2 (12) Identification and Authentication (Organization Users) | Acceptance of PIV Credentials

|  |
| --- |
| **IA-2 (12) Requirement(s)** |
| The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.  IA-2 (12) Additional FedRAMP Requirements and Guidance:  Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12. |
| **IA-2 (12) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IA-2 (12) What is the solution and how is it implemented?** |
| Description of how IA-2 (12) is implemented.  Customer Responsibilities |
| **IA-2 (12) Assessment Plan/Procedures** |
| **Assessment Objectives**  Determine if the information system:   * Accepts PIV credentials. * Electronically verifies PIV credentials.   **Assessment Procedures**   * Examine - Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; and other relevant documents or records. * Interview - Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; and system developers. * Test - Automated mechanisms supporting and/or implementing acceptance and verification of PIV credentials. |
| **IA-2 (12) Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IA-2(12) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### IA-5(11) Identification and Authentication (Organization Users) | Hardware Token-Based Authentication

|  |
| --- |
| **IA-5(11) Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IA-5(11) What is the solution and how is it implemented?** |
| Description of how IA-5(11) is implemented.  Customer Responsibilities |
| **IA-5(11) Assessment Plan/Procedures** |
| **Assessment Objectives**  Determine if, for hardware token-based authentication, the organization:   * Defines token quality requirements to be satisfied. * Employs mechanisms that satisfy organization-defined token quality requirements.   **Assessment Procedures**   * Examine - Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; automated mechanisms employing hardware token-based authentication for the information system; list of token quality requirements; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. * Interview - Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; and system developers. * Test - Automated mechanisms supporting and/or implementing hardware token-based authenticator management capability. |
| **IA-5(11) Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IA-5(11) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### Control IA-6 Authenticator Feedback

|  |
| --- |
| **IA-6 Requirement(s)** |
| The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. |
| **IA-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IA-6 What is the solution and how is it implemented?** |
| Description of how IA-6 is implemented.  Customer Responsibilities |
| **IA-6 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.  **Assessment Procedures**   * Examine - Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. * Interview - Organizational personnel with information security responsibilities; system/network administrators; and system developers. * Test - Automated mechanisms supporting and/or implementing the obscuring of feedback of authentication information during authentication. |
| **IA-6 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IA-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### IA-8(1) Identification and Authentication (Non-Organization Users) | Acceptance of PIV Credentials from Other Agencies

|  |
| --- |
| **IA-8(1) Requirement(s)** |
| The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. |
| **IA-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IA-8(1) What is the solution and how is it implemented?** |
| Description of how IA-8(1) is implemented.  Customer Responsibilities |
| **IA-8(1) Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the information system:   * Accepts PIV credentials from other agencies. * Electronically verifies PIV credentials from other agencies.   **Assessment Procedures**   * Examine - Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; and other relevant documents or records. * Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; and organizational personnel with account management responsibilities. * Test - Automated mechanisms supporting and/or implementing identification and authentication capability; automated mechanisms that accept and verify PIV credentials. |
| **IA-8(1) Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IS-8(1) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### IA-8(2) Identification and Authentication (Non-Organization Users) | Acceptance of Third-Party Credentials

|  |
| --- |
| **IA-8(2) Requirement(s)** |
| The information system accepts only FICAM-approved third-party credentials. |
| **IA-8(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IA-8(2) What is the solution and how is it implemented?** |
| Description of how IA-8(2) is implemented.  Customer Responsibilities |
| **IA-8(2) Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the information system accepts only FICAM-approved third-party credentials.  **Assessment Procedures**   * Examine - Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of FICAM-approved, third-party credentialing products, components, or services procured and implemented by organization; third-party credential verification records; evidence of FICAM-approved third-party credentials; third-party credential authorizations; and other relevant documents or records. * Interview - Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; and organizational personnel with account management responsibilities. * Test - Automated mechanisms supporting and/or implementing identification and authentication capability; automated mechanisms that accept FICAM-approved credentials. |
| **IA-8(2) Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IS-8(2) Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Incident Response (IR)

### IR-4 Incident Handling

|  |
| --- |
| **IR-4 Requirement(s)** |
| The organization:   1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; 2. Coordinates incident handling activities with contingency planning activities; and 3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.   **Additional FedRAMP Requirements and Guidance:** **Requirement:** The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system. |
| **IR-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IR-4 What is the solution and how is it implemented?** |
| Description of how IR-4 is implemented.  Customer Responsibilities |
| **IR-4 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Implements an incident handling capability for security incidents that includes: * Preparation; * Detection and analysis; * Containment; * Eradication; and * Recovery. * Coordinates incident handling activities with contingency planning activities. * Incorporates lessons learned from ongoing incident handling activities into: * Incident response procedures; * Training; and * Testing/exercises. * Implements the resulting changes accordingly to:   + Incident response procedures;   + Training; and   + Testing/exercises.   **Assessment Procedures**   * Examine - Incident response policy; contingency planning policy; procedures addressing incident handling; incident response plan; contingency plan; security plan; and other relevant documents or records. * Interview - Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; and organizational personnel with information security responsibilities. * Test - Incident handling capability for the organization |
| **IR-4 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IR-4 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### IR-6 Incident Reporting

|  |
| --- |
| **IR-6 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **IR-6 What is the solution and how is it implemented?** |
| Description of how IR-6 is implemented.  Customer Responsibilities |
| **IR-6 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines the time period within which personnel report suspected security incidents to the organizational incident response capability. * Requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period. * Defines authorities to whom security incident information is to be reported. * Reports security incident information to organization-defined authorities.   **Assessment Procedures**   * Examine -Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; security plan; and other relevant documents or records. * Interview - Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities; personnel who have/should have reported incidents; and personnel (authorities) to whom incident information is to be reported. * Test - Organizational processes for incident reporting; automated mechanisms supporting and/or implementing incident reporting |
| **IR-6 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **IR-6 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Planning (PL)

### PL-2 System Security Plan

|  |
| --- |
| **PL-2 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **PL-2 What is the solution and how is it implemented?** |
| Description of how PL-2 is implemented.  Customer Responsibilities |
| **PL-2 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Develops a security plan for the information system that: * Is consistent with the organization’s enterprise architecture;   + Explicitly defines the authorization boundary for the system;   + Describes the operational context of the information system in terms of missions and business processes;   + Provides the security categorization of the information system including supporting rationale;   + Describes the operational environment for the information system and relationships with or connections to other information systems;   + Provides an overview of the security requirements for the system;   + Identifies any relevant overlays, if applicable;   + Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and   + Is reviewed and approved by the authorizing official or designated representative prior to plan implementation. * Defines personnel or roles to whom copies of the security plan are to be distributed and subsequent changes to the plan are to be communicated. * Distributes copies of the security plan and communicates subsequent changes to the plan to organization-defined personnel or roles. * Defines the frequency to review the security plan for the information system. * Reviews the security plan for the information system with the organization-defined frequency. * Updates the plan to address:   + Changes to the information system/environment of operation;   + Problems identified during plan implementation; and   + Problems identified during security control assessments. * Protects the security plan from unauthorized:   + Disclosure; and   + Modification.   **Assessment Procedures**   * Examine -Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; and other relevant documents or records. * Interview - Organizational personnel with security planning and plan implementation responsibilities; and organizational personnel with information security responsibilities. * Test - Organizational processes for security plan development/review/update/approval; automated mechanisms supporting the information system security plan. |
| **PL-2 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **PL-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Personnel Security (PS)

### PS-3 Personnel Screening

|  |
| --- |
| **PS-3 Requirement(s)** |
| The organization:   1. Screens individuals prior to authorizing access to the information system; and 2. Rescreens individuals according to [*FedRAMP* *Assignment: for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.*] |
| **PS-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **PS-3 What is the solution and how is it implemented?** |
| Description of how PS-3 is implemented.  Customer Responsibilities |
| **PS-3 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Screens individuals prior to authorizing access to the information system. * Defines conditions requiring re-screening. * Defines the frequency of re-screening where it is so indicated. * Re-screens individuals in accordance with organization-defined conditions requiring re-screening and, where re-screening is so indicated, with the organization-defined frequency of such re-screening.   **Assessment Procedures**   * Examine - Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; and other relevant documents or records. * Interview -Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities. * Test - Organizational processes for personnel screening. |
| **PS-3 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **PS-3Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## Risk Assessment (RA)

### RA-2 Security Categorization

|  |
| --- |
| **RA-2 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **RA-2 What is the solution and how is it implemented?** |
| Description of how RA-2 is implemented  Customer Responsibilities |
| **RA-2 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Categorizes information and the information system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. * Documents the security categorization results (including supporting rationale) in the security plan for the information system. * Ensures the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.   **Assessment Procedures**   * Examine - Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and information systems; security plan; security categorization documentation; and other relevant documents or records. * Interview - Organizational personnel with security categorization and risk assessment responsibilities; and organizational personnel with information security responsibilities. * Test - Organizational processes for security categorization. |
| **RA-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **RA-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### RA-3 Risk Assessment

|  |
| --- |
| **RA-3 Requirement(s)** |
| The organization:   1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; 2. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*FedRAMP Assignment: security assessment report*]]; 3. Reviews risk assessment results [*FedRAMP Assignment: at least every three years or when a significant change occurs*]; 4. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and 5. Updates the risk assessment [*FedRAMP Assignment: at least every three years or when a significant change occurs*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.   **RA-3 Additional FedRAMP Requirements and Guidance:** **Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F  **RA-3d Additional FedRAMP Requirements and Guidance:** **Requirement:** Requirement to include the Authorizing Official; for JAB authorizations to include FedRAMP. |
| **RA-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **RA-3 What is the solution and how is it implemented?** |
| Description of how RA-3 is implemented  Customer Responsibilities |
| **RA-3 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * 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. * 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 the system processes, stores, or transmits. * Defines a document in which risk assessment results are to be documented (if not documented in the security plan or risk assessment report). * Documents risk assessment results in one of the following:   + The security plan;   + The risk assessment report; or   + The organization-defined document. * Defines the frequency to review risk assessment results. * Reviews risk assessment results with the organization-defined frequency. * Defines personnel or roles to whom risk assessment results are to be disseminated. * Disseminates risk assessment results to organization-defined personnel or roles. * Defines the frequency to update the risk assessment. * Updates the risk assessment:   + With the organization-defined frequency;   + Whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities); and   + Whenever there are other conditions that may impact the security state of the system.   **Assessment Procedures**   * Examine - Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; and other relevant documents or records. * Interview -Organizational personnel with risk assessment responsibilities; and organizational personnel with information security responsibilities. * Test -Organizational processes for risk assessment; automated mechanisms supporting and/or for conducting, documenting, reviewing, disseminating, and updating the risk assessment. |
| **RA-3 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **RA-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### RA-5 Vulnerability Scanning

|  |
| --- |
| **RA-5 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **RA-5 What is the solution and how is it implemented?** |
| Description of how RA-5 is implemented.  Inherited Services information  Customer Responsibilities |
| **RA-5 Assessment Plan/Procedures** |
| **FedRAMP DEFINED**  **Assessment Objectives**  Determine if the organization:   * Defines the frequency for conducting vulnerability scans on the information system and hosted applications. * Defines the process for conducting random vulnerability scans on the information system and hosted applications. * In accordance with the organization-defined frequency and/or organization-defined process for conducting random scans, scans for vulnerabilities in:   + The information system; and   + Hosted applications. * When new vulnerabilities potentially affecting the system/applications are identified and reported, scans for vulnerabilities in: * The information system; and * Hosted applications. * Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: * Enumerating platforms; * Enumerating software flaws; and * Enumerating improper configurations. * Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: * Formatting checklists; and * Formatting test procedures. * Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:   + Measuring vulnerability impact. * Analyzes vulnerability scan reports. * Analyzes results from security control assessments. * Defines response times to remediate legitimate vulnerabilities in accordance with an organizational assessment of risk. * Remediates legitimate vulnerabilities within the organization-defined response times in accordance with an organizational assessment of risk. * Defines personnel or roles with whom information obtained from the vulnerability scanning process and security control assessments is to be shared. * Shares information obtained from the vulnerability scanning process with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). * Shares information obtained from security control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).   **Assessment Procedures**   * Examine - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; and other relevant documents or records. * Interview - Organizational personnel with risk assessment, security control assessment and vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with vulnerability remediation responsibilities; organizational personnel with information security responsibilities; system/network administrators. * Test - Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing. |
| **RA-5 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **RA-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## System and Services Acquisition (SA)

### SA-9 External Information System Services

|  |
| --- |
| **SA-9 Requirement(s)** |
| The organization:   1. Requires that providers of external information system services comply with organizational information security requirements and employ [*FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; 2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and; 3. Employs [*FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored*] to monitor security control compliance by external service providers on an ongoing basis. |
| **SA-9 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SA-9 What is the solution and how is it implemented?** |
| Description of how SA-9 is implemented.  Customer Responsibilities |
| **SA-9 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines security controls to be employed by providers of external information system services. * Requires that providers of external information system services comply with organizational information security requirements. * Requires that providers of external information system services employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. * Defines and documents government oversight with regard to external information system services. * Defines and documents user roles and responsibilities with regard to external information system services. * Defines processes, methods, and techniques to be employed to monitor security control compliance by external service providers. * Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.   **Assessment Procedures**   * Examine System and services acquisition policy; procedures addressing external information system services; procedures addressing methods and techniques for monitoring security control compliance by external service providers of information system services; acquisition contracts, service-level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; and other relevant documents or records. * Interview - Organizational personnel with system and services acquisition responsibilities; external providers of information system services; organizational personnel with information security responsibilities. * Test -Organizational processes for monitoring security control compliance by external service providers on an ongoing basis; automated mechanisms for monitoring security control compliance by external service providers on an ongoing basis. |
| **SA-9 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SA-9 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## System and Communications Protection (SC)

### SC-5 Denial of Service Protection (Conditional)

|  |
| --- |
| **SC-5 Requirement(s)** |
| 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SC-5 What is the solution and how is it implemented?** |
| Description of how SC-5 is implemented.  Customer Responsibilities |
| **SC-5 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines types of denial of service attacks or reference to source of such information for the information system to protect against or limit the effects. * Defines security safeguards to be employed by the information system to protect against or limit the effects of organization-defined types of denial of service attacks. * Protects against or limits the effects of the organization-defined denial or service attacks (or reference to source for such information) by employing organization-defined security safeguards.   **Assessment Procedures**   * Examine -System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; list of denial of services attacks requiring employment of security safeguards to protect against or limit effects of such attacks; list of security safeguards protecting against or limiting the effects of denial of service attacks; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. * Interview -System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer. * Test - Automated mechanisms protecting against or limiting the effects of denial of service attacks. |
| **SC-5 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SC-5 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement |

### SC-7 Boundary Protection

|  |
| --- |
| **SC-7 Requirement(s)** |
| The information system:   1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; 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: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SC-7 What is the solution and how is it implemented?** |
| Description of how SC-7 is implemented.  Customer Responsibilities |
| **SC-7 Assessment Plan/Procedures** |
| **Assessment Objectives**  Determine if the organization:   * Monitors communications at the external boundary of the information system. * Monitors communications at key internal boundaries within the system. * Controls communications at the external boundary of the information system. * Controls communications at key internal boundaries within the system. * Implements subnetworks for publicly accessible system components that are either:   + Physically separated from internal organizational networks; and/or   + Logically separated from internal organizational networks. * Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.   **Assessment Procedures**   * Examine - System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; information system audit records; and other relevant documents or records. * Interview - System/network administrators; and organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. * Test - Automated mechanisms implementing boundary protection capability. |
| **SC-7 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SC-7 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### SC-12 Cryptographic Key Establishment & Management

|  |
| --- |
| **SC-12 Requirement(s)** |
| The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].  **SC-12 Additional FedRAMP Requirements and Guidance**: **Guidance:** Federally approved cryptography. |
| **SC-12 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here>, Date of Authorization |
| **SC-12 What is the solution and how is it implemented?** |
| Description of how SC-12 is implemented.  Customer Responsibilities |
| **SC-12 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines requirements for cryptographic key:   + Generation;   + Distribution;   + Storage;   + Access; and   + Destruction. * Establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation, distribution, storage, access, and destruction.   **Assessment Procedures**   * Examine - System and communications protection policy; procedures addressing cryptographic key establishment and management; information system design documentation; cryptographic mechanisms; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. * Interview - System/network administrators; organizational personnel with information security responsibilities; and organizational personnel with responsibilities for cryptographic key establishment and/or management. * Test - Automated mechanisms supporting and/or implementing cryptographic key establishment and management. |
| **SC-12 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SC-12 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### SC-13 Use of Cryptography

|  |
| --- |
| **SC-13 Requirement(s)** |
| The information system implements [*FedRAMP Assignment:* *FIPS-validated or NSA-approved cryptograph]* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. |
| **SC-13 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SC-13 What is the solution and how is it implemented?** |
| Description of how SC-13 is implemented.  Customer Responsibilities |
| **SC-13 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines cryptographic uses. * Defines the type of cryptography required for each use. * Implements the organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.   **Assessment Procedures**   * Examine - System and communications protection policy; procedures addressing cryptographic protection; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS validated cryptographic modules; information system audit records; and other relevant documents or records. * Interview - System/network administrators; organizational personnel with information security responsibilities; system developer; and organizational personnel with responsibilities for cryptographic protection. * Test - Automated mechanisms supporting and/or implementing cryptographic protection. |
| **SC-13 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SC-13 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

## System and Information Integrity (SI)

### SI-2 Flaw Remediation

|  |
| --- |
| **SI-2 Requirement(s)** |
| The organization:   1. Identifies, reports, and corrects information system flaws; 2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; 3. Installs security-relevant software and firmware updates within [*FedRAMP* *Assignment: Within 30 days of release of updates*] of the release of the updates; and 4. Incorporates flaw remediation into the organizational configuration management process. |
| **SI-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SI-2 What is the solution and how is it implemented?** |
| Description of how SI-2 is implemented.  Customer Responsibilities |
| **SI-2 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Identifies information system flaws. * Reports information system flaws. * Corrects information system flaws. * Tests software updates related to flaw remediation for effectiveness and potential side effects before installation. * Tests firmware updates related to flaw remediation for effectiveness and potential side effects before installation. * Defines the time period within which to install security-relevant software updates after the release of the updates. * Defines the time period within which to install security-relevant firmware updates after the release of the updates. * Installs software updates within the organization-defined time period of the release of the updates. * Installs firmware updates within the organization-defined time period of the release of the updates. * Incorporates flaw remediation into the organizational configuration management process.   **Assessment Procedures**   * Examine -System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software and firmware updates to correct information system flaws; installation/change control records for security-relevant software and firmware updates; and other relevant documents or records. * Interview - System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for flaw remediation; and organizational personnel with configuration management responsibility. * Test -Organizational processes for identifying, reporting, and correcting information system flaws; organizational process for installing software and firmware updates; automated mechanisms supporting and/or implementing reporting, and correcting information system flaws; and automated mechanisms supporting an/or implementing testing software and firmware updates. |
| **SI-2 Assessment Results** |
| Description of observations and evidence  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SI-2 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### SI-3 Malicious Code Protection

|  |
| --- |
| **SI-3 Requirement(s)** |
| The organization:   1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; 2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; 3. Configures malicious code protection mechanisms to:    1. Perform periodic scans of the information system [*FedRAMP Assignment: at least weekly*] and real-time scans of files from external sources at [*FedRAMP Assignment to include endpoints*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and    2. [*FedRAMP Assignment: to include alerting administrator or defined security personnel*] in response to malicious code detection; and 4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. |
| **SI-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SI-3 What is the solution and how is it implemented?** |
| Description of how SI-3 is implemented.  Customer Responsibilities |
| **SI-3 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Employs malicious code protection mechanisms to detect and eradicate malicious code at information system:   + Entry points; and   + Exit points. * Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures (as identified in CM-1). * Defines a frequency for malicious code protection mechanisms to perform periodic scans of the information system. * Defines action to be initiated by malicious protection mechanisms in response to malicious code detection. * Configures malicious code protection mechanisms to:   + Perform periodic scans of the information system with the organization-defined frequency;   + Perform real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy. * Configures malicious code protection mechanisms to do one or more of the following:   + Block malicious code in response to malicious code detection;   + Quarantine malicious code in response to malicious code detection;   + Send alert to administrator in response to malicious code detection; and/or   + Initiate organization-defined action in response to malicious code detection. * Addresses the receipt of false positives during malicious code detection and eradication. * Addresses the resulting potential impact on the availability of the information system.   **Assessment Procedures**   * Examine - System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system design documentation; information system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; information system audit records; and other relevant documents or records * Interview - System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for malicious code protection; and organizational personnel with configuration management responsibility. * Test - Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; automated mechanisms supporting and/or implementing employing, updating, and configuring malicious code protection mechanisms; automated mechanisms supporting and/or implementing malicious code scanning and subsequent act. |
| **SI-3 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SI-3 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

### SI-4 Information System Monitoring

|  |
| --- |
| **SI-4 Requirement(s)** |
| 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 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for <CSP Name here> , Date of Authorization |
| **SI-4 What is the solution and how is it implemented?** |
| Description of how SI-4 is implemented.  Customer Responsibilities |
| **SI-4 Assessment Plan/Procedures** |
| **Assessment Objective**  Determine if the organization:   * Defines monitoring objectives to detect attacks and indicators of potential attacks on the information system. * Monitors the information system to detect, in accordance with organization-defined monitoring objectives:   + - Attacks; and/or     - Indicators of potential attacks. * Monitors the information system to detect unauthorized:   + - Local connections;     - Network connections; and/or   + Remote connections. * Defines techniques and methods to identify unauthorized use of the information system. * Identifies unauthorized use of the information system through organization-defined techniques and methods. * Deploys monitoring devices:   + Strategically within the information system to collect organization-determined essential information.     - At ad hoc locations within the system to track specific types of transactions of interest to the organization. * Protects information obtained from intrusion-monitoring tools from unauthorized:   + - Access;     - Modification; and/or       * Deletion. * 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. * Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. * Defines personnel or roles to whom information system monitoring information is to be provided. * Defines information system monitoring information to be provided to organization-defined personnel or roles. * Defines a frequency to provide organization-defined information system monitoring to organization-defined personnel or roles. * Provides organization-defined information system monitoring information to organization-defined personnel or roles one or more of the following:   + - * As needed; and/or       * With the organization-defined frequency.   **Assessment Procedures**   * Examine - Continuous monitoring strategy; system and information integrity policy; procedures addressing information system monitoring tools and techniques; facility diagram/layout; information system design documentation; information system monitoring tools and techniques documentation; locations within information system where monitoring devices are deployed; information system configuration settings and associated documentation; and other relevant documents or records. * Interview -System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; and organizational personnel with responsibility monitoring the information system. * Test - Organizational processes for information system monitoring; automated mechanisms supporting and/or implementing information system monitoring capability. |
| **SI-4 Assessment Results** |
| Description of observations and evidence.  Final status: Implemented/Other than implemented  If other than implemented, description of weakness and risk to the system. |
| **SI-4 Remediation Plan** |
| Define remediation plans to correct risks identified with this control requirement. |

# Summary of Assessment Results

The assessment took place between <*date*> and <*date*>. The assessment was conducted in accordance with the assessment plans/procedures defined in this FedRAMP *Tailored* LI-SaaS Framework. All assessment activities documented to occur as described in the assessment plan <*did / did not*> take place as described. <*describe exceptions as applicable*>.

Table 15.1, Summary of Risks, represents the aggregate risk identified from the FedRAMP assessment. High risks are <*number*>% of total risks for the system. Moderate risks are<*number*>% of total risks for the system. Low risks are <*number*>% of total risks for the system. There <*are/ are not*> risks identified that are required for continued operation of the system.

Table .. Summary of Risks

|  |  |  |
| --- | --- | --- |
| **Risk Category** | **Total** | **% of Total Risks** |
| High |  | XX% |
| Moderate |  | XX% |
| Low |  | XX% |
| Operationally Required |  | XX% |
| **Total Risks[[19]](#footnote-19)** |  | 100% |

The summary is contained in the following embedded file:



**Assessment Teams**

The security assessment team consists of individuals from *<Independent Assessor>* that are located at the following address: *< Name>* <*Address*>.

The members of the independent assessor security testing team are in Table 15.2, below.

Table .. <Independent Assessor Name> FedRAMP Tailored LI-SaaS CSP Team Members

| **Name** | **Role** | **Contact Information** |
| --- | --- | --- |
| Enter Test Team POC Name | Enter Test Team POC Role | Enter Test Team Contract Information |
| Enter Test Team POC Name | Enter Test Team POC Role | Enter Test Team Contract Information |
| Enter Test Team POC Name | Enter Test Team POC Role | Enter Test Team Contract Information |

The <CSP Name> members of the testing team are listed in Table 15.3, below.

Table .. <CSP Name> FedRAMP Tailored LI-SaaS CSP Team Members

| Name | Role | Contact Information |
| --- | --- | --- |
| Enter CSP POC Name | Enter CSP POC Role | Enter CSP Contact Information |
| Enter CSP POC Name | Enter CSP POC Role | Enter CSP Contact Information |
| Enter CSP POC Name | Enter CSP POC Role | Enter CSP Contact Information |

# Summary of Remediation Plans

The following table provides a summary of the CSP plans for remediation and/or mitigation of risks identified in the assessment. The table will provide the initial plans for remediation as part of the risk-based decision by the AO for issuing an ATO.

This table will be updated with current status of open and new vulnerabilities on a monthly basis and provided to the AO as a component of continuous monitoring of the ongoing risk posture. At a minimum, the table must include the following information:

* Unique item number
* Reference item number from initial assessment, as applicable
* Weakness description
* Source of discovery [e.g., scan type]
* Date of discovery
* Security Impact Level (high, moderate, low)
* Planned date for remediation
* Revised date for remediation, if applicable
* Current status (open, closed)
* Comments (additional information, as applicable)

This information is required to be provided as Attachment 4 to this document.

# Acronyms

Refer to the *FedRAMP Master Acronym and Glossary* document available on the FedRAMP website (<https://www.fedramp.gov/resources/documents-2016/>).

# ATTACHMENTS

*Instruction: Attach any documents that are referred to in this FedRAMP* Tailored *LI-SaaS Framework. Documents and attachments should, provide the title, version, and exact file name, including the file extension.*

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

## Recommended Attachment File Naming Convention

A recommended attachment file naming convention is provided in the following table, Attachment File Naming Convention. Use this to generate names for the attachment files.

Table .. Attachment File Naming Convention

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Attachment** | **File Name** | **File Extension** |
| **1** | FedRAMP *Tailored* LI-SaaS CIS Worksheet | <*(Information System Abbreviation)* CIS version X> | . enter extension |
| **2** | FedRAMP Inventory Workbook | <*(Information System Abbreviation)* Inventory version X> | . enter extension |
| **3** | FedRAMP FIPS 199 | <Information System FIPS 199 version X> | . enter extension |
| **4** | <CSP/System Name> Summary of Remediation Plans | <*(Information System Abbreviation)* Remediation Plans version X> | . enter extension |
|  | Additional attachments as applicable |  |  |

## ATTACHMENT 1 – FedRAMP *Tailored* LI-SaaS CIS Worksheet

*All Authorization Packages must include the FedRAMP Control Implementation Summary (CIS) Worksheet. The template is provided in the following file:*

The following file includes a summary of the control implementation information provided in this FedRAMP *Tailored* LI-SaaS Framework:



## ATTACHMENT 2 – FedRAMP Inventory Workbook

All Authorization Packages must include a complete inventory. The FedRAMP Inventory Workbook can be found at the following FedRAMP website page: (<https://www.fedramp.gov/resources/templates-2016/>)

## ATTACHMENT 3 – FedRAMP FIPS 199 Security Categorization

All Authorization Packages must include a complete FIPS 199. The FedRAMP FIPS 199 Template can be found at the following FedRAMP website page: (<https://www.fedramp.gov/resources/templates-2016/>)

## ATTACHMENT 4 – <CSP/System Name> Summary of Remediation Plans

List all the risks and vulnerabilities identified as part of the assessment in a document entitled *<CSP/System Name> Summary of Remediation Plans* and provide it as Attachment 4 to this document.

## ATTACHMENT 5 – FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Self-Attestation Requirements

This document provides instructions and a template for completing the CSP self-attestation information for the applicable controls.

## ATTACHMENT 6 – FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Continuous Monitoring Plan

Refer to the FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Guide for information about implementing and maintaining compliance with FedRAMP *Tailored* LI-SaaS continuous monitoring requirements.

1. FIPS Pub 199: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION: Standards for Security Categorization of Federal Information and Information Systems, February 2004; <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> [↑](#footnote-ref-1)
2. AC-7 - NSO for non-privileged users. Attestation for privileged users related to multi-factor identification and authentication. [↑](#footnote-ref-2)
3. CA-5 - Attestation - for compliance with FedRAMP *Tailored* LI-SaaS Continuous Monitoring Requirements (See Attachment 6, FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Continues Monitoring Guide) l. [↑](#footnote-ref-3)
4. CA-9- Required - Conditional - Control is applicable if there are internal system connection(s). Connections (if any) shall be authorized and: 1) Identify the interface/connection; 2) Detail what data is involved and its sensitivity; 3) State whether the connection is one-way or bidirectional; and, 4) Describe how the connection is secured. [↑](#footnote-ref-4)
5. CM-6 - Required - Specifically include details of least functionality. [↑](#footnote-ref-5)
6. IA-2 - NSO for non-privileged users. Attestation for privileged users related to multi-factor identification and authentication. Specifically include description of management of service accounts. [↑](#footnote-ref-6)
7. IA-2(12) - Required (Conditional) - Required for privileged users; conditional for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP. [↑](#footnote-ref-7)
8. IA-5(11) - FED - for Federal privileged users; Required (Conditional) - Required for privileged users; conditional for all non-privileged users. [↑](#footnote-ref-8)
9. IA-8(1) - Required (Conditional) - Required for privileged users; conditional for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP. [↑](#footnote-ref-9)
10. IA-8(2) - Required (Conditional) - Required for privileged users; conditional for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP. [↑](#footnote-ref-10)
11. IR-8 - Attestation - Specifically attest to US-CERT compliance. [↑](#footnote-ref-11)
12. IR-9 - Attestation - Specifically describe information spillage response processes. [↑](#footnote-ref-12)
13. MA-2, 4 - attested if inherited from a FedRAMP authorized IaaS or PaaS. Required otherwise. [↑](#footnote-ref-13)
14. MP-2, 6, 7 - attested if inherited from a FedRAMP authorized IaaS or PaaS. Required otherwise. [↑](#footnote-ref-14)
15. PE-2, 3, 6, 8, 12, 13, 14, 15 and 16 - attested if inherited from a FedRAMP authorized IaaS or PaaS. Required otherwise. [↑](#footnote-ref-15)
16. SC-5 - Required: (Conditional) - If availability is a requirement - define protections in place as per control requirement. [↑](#footnote-ref-16)
17. SC-13 - Required: (Conditional) - if implementing, need to detail how they meet it or don't meet it. [↑](#footnote-ref-17)
18. SI-12 - Attestation - specifically related to US-CERT and FedRAMP communications procedures. [↑](#footnote-ref-18)
19. Total is the sum of High, Moderate, and Low with Operationally Required represented as a subset of this total. [↑](#footnote-ref-19)