|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | FedRAMP® <Choose: High, Moderate, Low, LI-SaaS> Baseline System Security Plan (SSP)  for <Insert CSP Name>  <Insert CSO Name>  <Insert Version X.X>  <Insert MM/DD/YYYY> | |  |
|
|  |  | |  |
|  |  | Controlled Unclassified Information info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/30/2023 | 1.0 | All | Initial publication after combining "front matter" sections of the FedRAMP System Security Plan (SSP) High Baseline Template, FedRAMP System Security Plan (SSP) Moderate Baseline Template, FedRAMP System Security Plan (SSP) Low Baseline Template, and Appendix B - FedRAMP Tailored LI-SaaS Template. | FedRAMP PMO |
|  |  |  |  |  |

**How to contact us**

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

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

Delete this Template Revision History page and all other instructional text from your final version of this document.

|  |
| --- |
| ***Instructions:*** |
| *Before populating this template, the FedRAMP PMO recommends reviewing the* [CSP Authorization Playbook: Getting Started with FedRAMP](https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook_Getting_Started_with_FedRAMP.pdf) *(Volumes I and II) and the* [Agency Authorization Playbook](https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf). *These* *documents provide a great starting point for new stakeholders and a reference resource for seasoned stakeholders.*  *This System Security Plan (SSP) template addresses all FedRAMP baselines; High, Moderate, Low, and Low-Impact Software as a Service (LI-SaaS). Sections 1 through 12 must be completed for all baselines. Beyond Section 12, some of the appendices change, depending on the impact level of the cloud service offering (CSO). For example, each impact level has a separate “Security Controls” Appendix (Appendix A) that includes the applicable controls for the particular security baseline. Additionally, some of the appendices are not required for LI-SaaS CSOs.*  *In the sections that follow, describe the system, the service offering components and features, and its security posture in the relevant diagrams, tables, and security controls. Instructions are offered in each section. There are several sections that include tables which may grow disproportionately with the Word document itself. You may remove the table from the section and add it as an additional appendix to the SSP.* *Be sure to replace the template text with “****<Insert Table #> is provided in <Insert Appendix letter>****,” and include a hyperlink to the appendix.*  *Once you begin populating this template it becomes a draft. The word “template” can be removed wherever it appears. As you go through the template entering data, you will see prompts for you to enter different types of data. There are no repeatable fields in this template. Please ensure that the inserted wording makes grammatical sense, as applied.*  ***Date Selection***  *Data items that must contain a date will present a date field to fill in (i.e., mm/dd/yyyy).*  ***Item Choice***  *Data items may have a limited number of value choices, which are noted, in brackets, as choices.*  *Insert the appropriate choice.*  ***Instructional Text***  *Instructions are provided to help you understand how to complete this SSP template. Before delivering the final version of the SSP, be sure to delete all italicized instructional text.*  Delete this instructional text from your final version of this document. |

SYSTEM SECURITY PLAN

Prepared by

|  |  |
| --- | --- |
| Identification of Organization that Prepared this Document | |
| **Organization Name** | <Enter Company/Organization> |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |

Prepared for

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

Document Revision History

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

TABLE OF CONTENTS

[1 Introduction 8](#_Toc132928029)

[2 Purpose 8](#_Toc132928030)

[3 System Information 8](#_Toc132928031)

[4 System Owner 10](#_Toc132928032)

[5 Assignment of Security Responsibility 11](#_Toc132928033)

[6 Leveraged FedRAMP-Authorized Services 12](#_Toc132928034)

[7 External Systems and Services Not Having FedRAMP Authorization 15](#_Toc132928035)

[8 Illustrated Architecture and Narratives 19](#_Toc132928036)

[8.1 Illustrated Architecture 19](#_Toc132928037)

[8.2 Narrative 22](#_Toc132928038)

[9 Services, Ports, and Protocols 24](#_Toc132928039)

[10 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) 27](#_Toc132928040)

[11 Separation of Duties 29](#_Toc132928041)

[12 SSP Appendices List 31](#_Toc132928042)

[Appendix A <Insert CSO Name> FedRAMP Security Controls 33](#_Toc132928043)

[Appendix B <Insert CSO Name> Related Acronyms 35](#_Toc132928044)

[Appendix C <Insert CSO Name> Information Security Policies and Procedures 36](#_Toc132928045)

[Appendix D <Insert CSO Name> User Guide 37](#_Toc132928046)

[Appendix E <Insert CSO Name> Digital Identity Worksheet 37](#_Toc132928047)

[Appendix F <Insert CSO Name> Rules of Behavior (RoB) 40](#_Toc132928048)

[Appendix G <Insert CSO Name> Information System Contingency Plan (ISCP) 40](#_Toc132928049)

[Appendix H <Insert CSO Name> Configuration Management Plan (CMP) 41](#_Toc132928050)

[Appendix I <Insert CSO Name> Incident Response Plan (IRP) 42](#_Toc132928051)

[Appendix J <Insert CSO Name> Control Implementation Summary (CIS) and Customer Responsibilities Matrix (CRM) Workbook 43](#_Toc132928052)

[Appendix K <Insert CSO Name> Federal Information Processing Standard (FIPS) 199 Categorization 44](#_Toc132928053)

[Appendix L <Insert CSO Name>-Specific Laws and Regulations 47](#_Toc132928054)

[Appendix M <Insert CSO Name> Integrated Inventory Workbook (IIW) 47](#_Toc132928055)

[Appendix N <Insert CSO Name> Continuous Monitoring Plan 48](#_Toc132928056)

[Appendix O <Insert CSO Name> POA&M 49](#_Toc132928057)

[Appendix P <Insert CSO Name> Supply Chain Risk Management Plan (SCRMP) 49](#_Toc132928058)

[Appendix Q <Insert CSO Name> Cryptographic Modules Table 50](#_Toc132928059)

SYSTEM SECURITY PLAN APPROVALS

|  |
| --- |
| ***Instructions:*** |
| *Add or remove signature boxes, as needed. Digital or wet/physical signatures are permitted.*  Delete this and all other instructional text from your final version of this document. |

**Cloud Service Provider (CSP) Signatures**

By signing this System Security Plan (SSP), we agree that it is complete and is the current version to be used for the security assessment. [The FedRAMP-specific Laws and Regulations Document](https://www.fedramp.gov/assets/resources/templates/SSP-A12-FedRAMP-Laws-and-Regulations-Template.xlsx), as of the date of this SSP, is <Insert Version X.X>, dated <Insert MM/DD/YYYY>, and is posted on the [FedRAMP Documents and Templates webpage](https://www.fedramp.gov/documents-templates/). The CSO-related laws and regulations, beyond those required by FedRAMP, are captured in Appendix L.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | | | | |
|  | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | | | | |
|  | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | |  | | |

# Introduction

The SSP is the “security blueprint” of a CSO. The SSP defines a CSO’s authorization boundary and describes the security controls in place to protect the confidentiality, integrity, and availability (CIA) of the system and federal data it holds.

# Purpose

This document is intended to be used by CSPs that are pursuing a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO) or an agency authorization to operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).

# System Information

|  |
| --- |
| ***Instructions:*** |
| *Complete Table 3.1 as indicated. The Digital Identity Level and FIPS PUB 199 Level should be completed after completing the corresponding appendices and determining appropriate content.*   * ***Service Model:*** *Choose Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Low-Impact Software as a Service (LI-SaaS), or some combination of these.* * ***Fully Operational as of:*** *“Fully operational” means there are no “gaps” in the security control baseline implementations for the system. The CSP attests that the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.* * ***Deployment Model:*** *See the FedRAMP CSP Playbook, Volume I, Section 7 (Deployment Models) for definitions of the deployment models and make selection based on intended use case.*    + *For* ***Hybrid*** *Cloud, in the “General System Description”, describe how the service solution varies. For example, if part of the solution is provided for a single agency (private cloud) and part is provided for several agencies (government-only community).* * *For* ***Government-only Community*** *Cloud, in the “General System Description”, define the members of the community (e.g., any combination of federal in addition to state government, local government, tribal government, research institutions, federal contractors, or government contractors).* * ***General System Description****: Provide a description of all services and features that are included as part of this CSO and within the authorization boundary. The description should only include those items inside the service boundary that have been independent assessor (IA) tested as part of this assessment.* ***This general description will be the service description that is used on the FedRAMP Marketplace.*** *Keep in mind the following:* * *A service description should incorporate the functional characteristics of a CSO.* * *A service description should not include marketing language and is not meant to be a place where a company should be promoting or showcasing company accomplishments.* * *A service description should provide a representation of the services, features or components that have been tested and accredited as part of a CSO’s authorization boundary.* * *A service description should note the intended user base specifics, as indicated above, for Hybrid and Government-only Community Cloud CSOs.*   Delete this and all other instructional text from your final version of this document. |

Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

|  |  |
| --- | --- |
| System Information | |
| **CSP Name:** | <Insert CSP Name> <Insert CSP Abbreviation, as appropriate> |
| **CSO Name:** | <Insert CSO Name> <Insert CSO Abbreviation, as appropriate> |
| **FedRAMP Package ID:** | <Insert FedRAMP Package ID> |
| **Service Model:** | <Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS> |
| **Digital Identity Level (DIL) Determination (SSP Appendix E):** | <Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1> |
| **FIPS PUB 199 Level (SSP Appendix K):** | <Choose one: High, Moderate, Low, LI-SaaS> |
| **Fully Operational as of:** | <Insert MM/DD/YYYY> |
| **Deployment Model:** | <Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud> |
| **Authorization Path:** | <Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization> |
| **General System Description:** | <Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)]. |

# System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system. The system owner is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Table 4.1 <Insert CSO Name> Owner

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

# Assignment of Security Responsibility

|  |
| --- |
| ***Instructions:*** |
| *Complete Table 5.1 as indicated. If there are other personnel with key security responsibilities for the CSO, additional tables may be added.*  *The Information System Security Officer (ISSO) is the individual who is assigned responsibility for maintaining the appropriate operational security posture for an information system or program.*  Delete this and all other instructional text from your final version of this document. |

The <Insert CSP Name> <Insert CSO Name> Information System Security Officer (ISSO), or equivalent, identified below, has been ***appointed in writing*** and is deemed to have significant cyber security and operational role responsibilities.

Table 5.1 <Insert CSP Name> ISSO (or Equivalent) Point of Contact

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

# Leveraged FedRAMP-Authorized Services

|  |
| --- |
| ***Instructions:*** |
| *Table 6.1 includes all functions, services, features, and APIs that are leveraged from FedRAMP Authorized CSOs. The FedRAMP Marketplace is the authoritative source for identifying CSOs and their services that are FedRAMP Authorized.*  *Alternatively, you may remove the below table and add it as an additional appendix to the SSP. Be sure to replace the template text with* ***“The <Insert CSO Name> leverages the FedRAMP Authorized services depicted in <Insert Appendix Letter>,”*** *and include a hyperlink to the appendix.*  *When completing the table, please note the following:*   * *The leveraged “CSP and CSO Name” must be listed on the FedRAMP Marketplace with a status of “Authorized.”*   + *“In Process” and “FedRAMP Ready” designations are not equivalent to FedRAMP Authorized.* * *A “CSO Service” must also be derived from the FedRAMP Marketplace.*   + *Refer to the leveraged CSO’s FedRAMP Marketplace listing to verify services and features that are included in the CSO’s boundary. Services or features that are NOT included in the Marketplace listing (i.e., not FedRAMP Authorized) are considered “external services” and must be listed in Section 7, External Systems and Services Not Having FedRAMP Authorization.*   + *If the system is leveraging external services from a FedRAMP Authorized system, the interfaces to the services must be included in the boundary and must also be assessed by an independent assessor (IA) (e.g., if a CSO uses FedRAMP Service A from FedRAMP CSO B, FedRAMP CSO A interfaces must be tested and included in the authorization boundary). At a minimum, the CSP must address all the customer responsibilities defined by the external service in a FISMA compliant manner.*   + *Occasionally, CSOs leverage non-customer-facing, internal services from another authorized CSO by the same CSP. This is sometimes referred to as a “first-party” service. A typical example would be a CSP standing up a second CSO and using the scanning and logging capabilities of a previously FedRAMP Authorized CSO to support the new CSO. The CSP should clearly indicate this in the “CSO Service” column, and an IA should review the shared capability in the external CSO to determine if the sharing interface was sufficiently tested for this purpose.* * *“Nature of Agreement” is any type of agreement between a CSP and the leveraged CSP vendors who support products (e.g., End User Licensing Agreement (EULA), Service-Level Agreement (SLA), App License Agreement, Contract, etc.).* * *“Data Types” are the CSO data types transmitted to, stored, or processed by the system/service, including sensitive federal data/system data. This column is based on the NIST 800-60 Vol II data types for the system. Longer lists of data types and data categorizations may instead be included in an appendix.* * *“Authorized Users/Authentication” are the user roles (e.g., SecOps Engineers) authorized to access the service, and provide the authentication method.* * *CSPs seeking a JAB P-ATO must confirm acceptability of using any FedRAMP Authorized services that lack a JAB P-ATO with JAB technical representatives (TRs).* * *CSPs must be cognizant of the impact level of leveraged FedRAMP Authorized services. CSOs should leverage services at the same, or higher, impact level. As a general rule, the use of any services, at a lesser impact level than the service undergoing FedRAMP authorization, must be carefully scrutinized to ensure that federal data is adequately protected (e.g., a CSO processing High federal data, or sensitive system data, should not leverage a Moderate, Low, or LI-SaaS service to process or store High federal data or sensitive system data).*   *Additional instructions are provided in the header row of Table 6.1.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> leverages the FedRAMP Authorized services depicted in Table 6.1 below.

*Table 6.1 Leveraged FedRAMP Authorized Services*

| # | CSP/CSO Name (Name on FedRAMP Marketplace) | CSO Service (Names of services and features - services from a single CSO can be all listed in one cell) | Authorization Type (JAB or Agency) and FedRAMP Package ID # | Nature of Agreement | Impact Level (High, Moderate, Low, LI-SaaS) | Data Types | Authorized Users/Authentication |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# External Systems and Services Not Having FedRAMP Authorization

|  |
| --- |
| ***Instructions:*** |
| *FedRAMP Authorized services should be used, whenever possible, since their risk is defined. In some cases, CSPs establish connections to external systems and services that lack FedRAMP authorization to exchange data and information or augment system functionality and provide operational support services. This includes corporate systems and services that are not part of the authorization boundary. Since external services/systems lacking authorization have unknown risk, CSPs are required to provide details about the services/systems, in Table 7.1, to help authorizing officials understand the impact to the CIA of a CSO, and the federal data it holds, if the CIA of the external service/system is compromised.*  *FedRAMP defines a connection as any communication path used to push, pull, or exchange data and/or information, including application programming interfaces (APIs) (e.g., the collection of traffic information via a geo-location service API set or integration with a service via its API set are both considered connections). The table, below, must include all external services that are mentioned in the SSP narrative and controls.*  *Alternatively, you may remove the below table and add it as an additional appendix to the SSP. Be sure to replace the template text with* ***"The <Insert CSO Name> makes use of systems, services, application program interfaces (APIs), and command-line interfaces (CLIs) lacking FedRAMP authorization as depicted in <Insert Appendix Letter>,"*** *and include a hyperlink to the appendix.*  *When completing the table, please note the following:*   * *Corporate services are those systems and services that are owned by the CSP in an environment controlled and operated by the CSP. They may include support services used exclusively by the CSO or that are shared with corporate users/resources. External cloud services used to support the corporate environment are not considered corporate services; since they are not under the full control of the CSP, such services are considered external cloud services. When corporate services are used, be sure to note:*   1. *Where the service is hosted (in a corporate data center or in another cloud)*   2. *The use case of the specific service and who has access to it* * *Identify all connections to external systems and services lacking FedRAMP authorization. Do not include the FedRAMP Authorized services listed in Table 6.1, above; there should be no overlap between these two tables.* * *Use the* [*FedRAMP Authorization Boundary Guidance*](https://www.fedramp.gov/assets/resources/documents/CSP_A_FedRAMP_Authorization_Boundary_Guidance_DRAFT.pdf) *when evaluating the use-case of all external systems or services. It is not acceptable to use unauthorized external systems, or services, for processing or storage of federal data or sensitive system data.* * *Connections to all external systems and services must be depicted on the authorization boundary, network, and data flow diagrams with directional arrows, as described in Section 8.*    1. *Directional arrows indicate the direction from where the initial connection is made (e.g., an external service initiates the contact and pushes data or the CSO initiates the contact and pulls data).*   2. *The narrative that accompanies the diagram(s) must clearly describe the flow of data and must correspond to the diagram.*   3. *Apply the same logic to all data flows internally, externally, and traversing the boundary.* * *The "Nature of Agreement" is any type of agreement between the CSP and the leveraged CSP vendors who support products (e.g., End User Licensing Agreement (EULA), Service-Level Agreement (SLA), App License Agreement, Contract, etc.).*   *Populate the columns in Table 7.1 as follows:*  ***System/Service/API/CLI Name (Non-FedRAMP Cloud Services)****: Provide the name of the system, service, API, or CLI. Include the vendor name, if different from the product name.*  ***Connection Details:*** *Provide connectivity details. Specifically, note whether inbound, outbound, or both.*  ***Nature of Agreement****: See the “Nature of Agreement” instructions above for Table 6.1.*  ***Still supported? Y or N****: Is this product still supported by the manufacturer?*  ***Data Types****: List the data types and metadata types transmitted to, stored, or processed by the system/service, including federal data and sensitive system data. This column is based on the NIST 800-60 Vol. II data types for the system. Longer lists of data types and data categorizations may instead be included in an appendix.*  ***Data Categorization****: Identify the security impact level of the data (Low, Moderate, High) in accordance with FIPS 199 & NIST 800-60 Vol. 2. Longer lists of data types and data categorizations may instead be included in an appendix.*  ***Authorized Users/Authentication****: List the user roles (e.g., SecOps engineers) authorized to access the service, and provide the authentication method.*  ***Other Compliance Programs****: List any certifications for this service (e.g., PCI SOC 2, CSA STAR Level 2, etc.), and provide the certification date. If FISMA authorized, that should also be specifically noted.*  ***Description****: Describe the purpose of the external system/service; specifically, provide reasons for connectivity (e.g., system monitoring, system alerting, download updates, etc.).*  ***Hosting Environment****: Describe the hosting environment (e.g., corporate network, IaaS, or self-hosted).*  ***Risk/Impact/ Mitigation****: Describe potential risks introduced by the external system/service and impact to the CSO or federal data if the CIA of the system/service is compromised. Describe any mitigations or compensating controls in place to reduce risk.*  *Delete this and all other instructional text from your final version of this document.* |

External systems/services, interconnections, application programming interfaces (APIs), and command line interfaces (CLIs) that do not have a FedRAMP authorization, at the same or greater impact level as <Insert CSO Name>, are described in Table 7.1 below.

Table 7.1 External Systems/Services, Interconnections, APIs, and CLIs Without FedRAMP Authorizations

| #  (either 1, 2, or 3)\*\* | System/ Service/ API/CLI Name (Non-FedRAMP Cloud Services) | Connection Details | Nature of Agreement | Still Supported? Y or N | Data Types | Data Categorization | Authorized Users/ Authentication | Other Compliance Programs | Description | Hosting Environment | Risk/Impact/ Mitigation |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

*\*\*1- Non-FedRAMP Authorized Cloud Services, 2- Corporate Shared Services, 3- Update Services for In-Boundary Software/Services*

# Illustrated Architecture and Narratives

|  |
| --- |
| ***Instructions:*** |
| *Use the* [FedRAMP Integrated Inventory Workbook](https://www.fedramp.gov/assets/resources/templates/SSP-A13-FedRAMP-Integrated-Inventory-Workbook-Template.xlsx) *template, and ensure the inventory items are named consistently, within the diagrams and within the narratives, in the sections that follow. Ensure naming conventions are adopted throughout the entire SSP (i.e., security control implementation descriptions and all attachments).*  *Delete this and all other instructional text from your final version of this document.* |

This section contains the diagrams and narratives for the <Insert CSO Name> authorization boundary, network, and data flows. Section 8.1 provides the diagrams, and Section 8.2 provides the associated narratives.

## Illustrated Architecture

|  |
| --- |
| ***Instructions:*** |
| *Choose the appropriate paragraph based on the number of diagrams; delete the other.*  *Delete this and all other instructional text from your final version of this document.* |

This section contains the diagram that represents the authorization boundary, network, and data flows. Following the diagram, there is a narrative that describes the <Insert CSO Name> boundary components, functionality, as well as interactions and flows among internal components and external systems/services.

or

This section contains the diagrams that represent the authorization boundary, network, and data flows. Following each of the diagrams, there is a narrative that describes the <Insert CSO Name> boundary components, functionality, as well as interactions and flows among internal components and external systems/services. If using several illustrations, each must have a narrative.

|  |
| --- |
| ***Instructions:*** |
| *In this section, provide the illustration(s) for the CSO’s authorization boundary, network architecture, and data flows. The illustration can be one all-encompassing diagram that addresses all required informational elements, or separate diagrams (Authorization Boundary Diagram [ABD], Network Diagram, Data Flow Diagram [DFD]) if there is concern about too much data on one diagram; however, if more than one diagram is used,* ***ALL diagrams must be consistent (using same component names, color coding, etc.) and represent at least the authorization boundary and its components****.*  ***Authorization Boundary Diagram****:*  *An acceptable ABD has a clearly marked boundary. Include a prominent border (e.g., a bold red line) around all systems and services included in the authorization boundary. The diagram must be legible and readable. Please note that some authorization boundary diagrams are large once all the required data and information has been included. In order to maintain high reading resolution for any of these supplied diagrams, FedRAMP asks that the CSP consider high resolution settings prior to saving the document. The CSP is reminded that the diagram can be made as large as possible and embedded into this document.*  *The diagram(s) should:*   * *Include a clearly defined authorization boundary (e.g. bold red line).* * *Include system interconnections used to operate and support the intended mission/business functions. Identify whether they are FedRAMP Authorized (or not).* * *Depict every tool, service, or component that is mentioned in the SSP narrative and controls.* * *Identify those depicted tools, services, or components as either external or internal to the boundary.* * *Clearly identify anywhere federal data is to be processed, stored, or transmitted.* * *Depict how the CSP and customer/agency access the service (e.g., the authentication used to access the service).* * *Depict all major software/virtual components (or groups of) within the boundary.* * *Depict all CSP-provided components that are deployed in customer environments that are within the boundary.* * *Be validated against the inventory.*   + *Component labels on diagrams should match corresponding entries in the "Diagram Label" column in the inventory workbook.*   + *The “Function” column in the inventory workbook should describe the function performed by the component within the CSO.*   + *All components internal to the CSO should appear both in the inventory and on the diagrams.*   + *It is understood that a single component on a diagram may represent many entries in the inventory.* * *Show an alternate processing site.* * *Show how updates are pulled from external services (e.g., the operating system (OS), antivirus software, etc.).*   ***Network Diagram:***  *If using a separate network overlay diagram, this should resemble the ABD and should include:*   * *Subnetworks* * *Location of DNS authoritative and recursive servers*   ***Data Flow Diagram:***  *If using a separate data flow overlay diagram, this should resemble the ABD, include the network components, and:*   * *Clearly identify data flows for privileged, non-privileged, and customers' access with MFA details.* * *Depict how all ports, protocols, and services of all internal and external traffic are represented and managed.* * *For each data flow, clearly depict protective mechanisms (i.e., the encryption type and FIPS 140-validation or use of other alternative implementations such as physical protection via protective distribution systems [PDS]), where applicable).* * *For each data store, clearly depict the encryption status (i.e., encrypted with FIPS 140 validated crypto modules, encrypted without FIPS, or unencrypted).The best approach is to use the reference # from the encryption tables below.*   *Refer to the latest* [*FedRAMP Authorization Boundary Guidance*](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj2ytTvz-f6AhUKMVkFHVyOCbQQFnoECC0QAQ&url=https%3A%2F%2Fwww.fedramp.gov%2Fassets%2Fresources%2Fdocuments%2FCSP_A_FedRAMP_Authorization_Boundary_Guidance_DRAFT.pdf&usg=AOvVaw347dZJFK19t5-1UA6-mt41) *available on the FedRAMP website.*  *Delete this and all other instructional text from your final version of this document.* |

## Narrative

|  |
| --- |
| ***Instructions:*** |
| ***NARRATIVE DESCRIPTION for the ABD, DFD, and Network Diagram:***  *Whether using one or multiple diagrams, after each, provide a detailed narrative description that clearly describes the CSO and the elements of the diagram. The narrative should describe the components of the system as depicted in the diagram using the same naming conventions, to avoid confusion. Additionally, the narrative must describe the relationships of the internal services. It may be useful to describe these using a numbering or lettering scheme and then include them in the diagram (i.e., enabling the narrative to act as a key for the diagram). Ensure to reference the diagram(s) by figure number in the narrative description, and name the diagram appropriately. If you choose to have separate diagrams, ensure that there is an appropriate narrative provided for each diagram.*  *Occasionally, there are other additional services being delivered from the same environment as the FedRAMP offering, that are* **excluded** *from independent assessor (IA) testing, and, therefore,* **excluded** *from the authorization boundary. This means that these additional services do not have a FedRAMP authorization and are a customer responsibility to accept the risk associated with using these non-FedRAMP Authorized services. The diagrams and narrative should clearly call this out. In addition, the narrative should indicate whether the CSP:*   * *Has plans for a near-term significant change to make these available to FedRAMP customers.*   *Or*   * *Has no plans to add these to this authorization boundary.*   ***The following narrative and optional table is offered as an example only to help CSPs understand the depth and breadth of the narratives that are required by FedRAMP.*** This example may be used as the basis to set up a narrative for a CSP.   * *<Insert CSO Name> is a government-community cloud environment that resides in the <Insert Name of IaaS/PaaS and Region> region. <Insert Name of IaaS/PaaS> has been granted a <insert JAB Provisional ATO (P-ATO) OR Agency ATO> for <Insert High, Moderate, Low, LI-SaaS> impact workloads.* * *<Insert CSO Name> has been implemented on <Insert Container Name> containers to provide a microservices-based architecture. The production environment includes applications, operating systems, and <Insert Name of IaaS/PaaS> resources and services that support this architecture. The major components include:*   + *Web services for access control as well as back-end processing nodes running <Insert Name of OS> or <Insert Name of OS> on <Insert Name of Service> instances, <Insert Name of OS> on containers managed using <Insert Name of Service>.*   + *Access control to the Web portal using <Insert Name of service(s)> service.*   + *Databases/Caching/Queuing:*     - *<Insert Name of Databases> databases installed on containers as the primary data store*     - *<Insert Name of Databases> for reports data*     - *<Insert Name of Database> for the metrics data*     - *<Insert Name of Service> for searching device metrics data*     - *<Insert Name of Service> for managed caching*     - *<Insert Name of Service> for data streaming*   + *Storage:*     - *<Insert Name of Service> volumes, which serve as block storage <Insert the Type of Storage> devices*     - *<Insert Name of Service> for <Insert Name of Service(s)>*     - *<Insert Name of Service>, which stores database backups; a separate <Insert Name of Service> stores audit logs from <Insert Name of Service>*   + *Networking:*     - *Virtual Private Cloud (VPC) with public and private subnets*     - *Route tables for traffic flow between subnets*     - *Security groups, which act as virtual firewalls*     - *<Insert Name of Service> for application load balancers (ALBs) and classic load balancers*     - *<Insert Name of Service> for external DNS*     - *<Insert Name of Service> for internal DNS*     - *<Insert Name of Service> for public certificates*     - *<Insert Name of Service> VPN for internal access to the environment*     - *<Insert Name of Service> for internal access between VPCs*   + *Management tools/services such as <Insert Name of of all Services>*     *Table 8.1 Security and Management Technologies*   |  |  | | --- | --- | | Category | Technical Solution / Vendor | | Operating Systems |  | | IAM/Access Management |  | | Endpoint/Antivirus (AV), File Integrity Monitoring (FIM) |  | | Code Repository |  | | Ticketing |  | | Configuration Management |  | | Firewall/VPN |  | | MFA |  | | SIEM |  | | Secrets Management |  | | Vulnerability Scanning |  |   *These components have been provisioned within two <Insert Name of Service> accounts (one for production and one for management) that are owned and managed by <Insert CSP Name>. The <Insert CSO Name> inventory is included in Appendix M, Integrated Inventory Workbook.*  *Delete this and all other instructional text from your final version of this document.* |

# Services, Ports, and Protocols

Table 9.1 lists the service names, port numbers, and transport protocols enabled in <Insert CSO Name>. These must be specifically called out per the security control requirements in CM-7, CM-7(1), RA-5, SA-4, SA-9(2), and SA-9(4).

|  |
| --- |
| ***Instructions:*** |
| ***Complete this table even if leveraging a pre-existing FedRAMP authorization.*** *Add more rows as needed. If you are unclear as to what should be included in this table, refer to:* <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>.  *Ensure that the services, ports, and protocols match the data collected in the rest of this SSP.*  *The developer of the system, system component, or system service is required to identify the functions, ports, protocols, and services intended for organizational use. This list must be kept current. It becomes resource-intensive to retrofit security controls after the system, component, or service has been implemented.*  ***Reference #:*** *Match this number to the reference number (“Ref #”) column in Appendix Q.*  ***Purpose:*** *Provide a general description of how it is used in the CSO, such as for Web access or database connection.*  ***Used By:*** *List the CSO components accessed by this port and the stated purpose.*  Delete this and all other instructional text from your final version of this document. |

Table 9.1 <Insert CSO Name> Services, Ports, and Protocols

| Service Name | Port # | Transport Protocol | Reference # | Purpose | Used By |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)

|  |
| --- |
| ***Instructions:*** |
| *Use the tables in Appendix Q to document the encryption status of all areas/flows of all data, to include: data at rest, data in transit across the boundary, data in transit within the boundary, remote access mechanisms (e.g., IPSec VPN), key management, key generation, underlying system config (e.g., running in FIPS mode), authentication, and digital signatures.*  *This section and its tables may be referenced in the control implementation description for SC-13 and other applicable controls (e.g., SC-8/SC-8(1) and SC-28/SC-28(1)). The reference numbers for the area of encryption, in the tables, should also be used in the SSP diagram(s) to provide readers a clear mapping of the CSO’s encryption status. The tables serve to greatly reduce the narrative required in the control(s) and diagrams, and they may also reduce extra remediation cycles due to questions from an IA, agency/JAB AO, and representatives from the FedRAMP PMO. For High baseline systems, please keep in mind that security control SI-7 (Software, Firmware, and Information Integrity) takes into account cryptographic hashes, which also must be created using FIPS-validated cryptographic modules.*  *If it is determined that there is an area that is either using a historical cryptographic module or that lacks encryption, a plan of action and milestones (POA&M) item should be created for each area, if one does not already exist. Additional details can be found in FedRAMP’s Security FAQ:* <https://www.fedramp.gov/faqs/#faq-security>.  *Since every encrypted connection has two ends, FedRAMP requires the source and destination for each connection. For an external service that lacks authorization, and the CSP is unaware of the type of encryption, choose “Unknown”. Keep in mind that the CSP should know the encryption on both ends of a connection to ensure that the data transmission is secure.*  *For Low services and LI-SaaS:*   1. *FIPS 140 validation is only mandatory for the MFA verifier.* 2. *When encryption is implemented, where not mandatory, the table should be used to document what is in place.*   *Add additional rows, as necessary, to account for all data at rest, data in transit across the boundary, data in transit within the boundary, remote access mechanisms (e.g., IPSec VPN), key management, key generation, underlying system configuration (e.g., running in FIPS mode), authentication, and digital signatures.*  *Delete this and all other instructional text from your final version of this document.* |

The use of cryptography is critical for all systems that process and/or store federal data. Federal policy requires that anywhere that cryptography is required, it must employ FIPS 140-validated cryptographic modules. The Appendix Q cryptographic modules tables specify the encryption status for <Insert CSO Name>. These tables include reference numbers that are specified in <Insert Figure Number(s) (refer to the diagrams in the SSP depicting encryption status, typically data flow, if not combined)> in Section 8 of this SSP that depict the specific data stores and flows related to <Insert CSO Name>.

<Insert CSP Name> confirms, except where clearly noted in Appendix Q, that <Insert CSO Name> employs FIPS-validated cryptographic modules (CMs) that are configured in an approved mode, which is documented in the associated Cryptographic Module Validation Program (CMVP) security policy for the FIPS-validated certificate number. Only algorithms listed, as approved, in the CM’s security policy are used. The encryption discussed, in Appendix Q, is validated by an IA during a security assessment.

# Separation of Duties

Security control AC-5, Separation of Duties, requires that CSPs identify and document the roles of ***all*** individuals who access the system and define the access authorizations that support protections from bad actors, employee collusion, fraud, etc. before damage occurs. Table 11.1 captures the roles and access privileges for all individuals or roles that access <Insert CSO Name>.

|  |
| --- |
| ***Instructions:*** |
| *In Table 11.1, identify and document all duty descriptions within the organization. Each duty description is listed in a separate row; if a CSP is a large and complex organization, there could be several. In the case of a CSP being large and complex, focus on the duty descriptions that apply to the CSO. There may be third party relationships that apply such as administrators who are not part of the organization; these should also be listed. Additionally, the table should include any duties performed by agency customers. Table 11.1 includes a few examples, which should be removed prior to populating this table for your CSO.*  *Identify and document all general roles for the organization or the CSO (one for each column); there may be indirect roles that apply that should also be listed.*  *If the CSO has many more duties and roles than what can fit within a table of this size, you may use an Excel spreadsheet and reference it as an appendix within the SSP and this section. Be sure to replace the template text with* ***"The <Insert CSO Name> Separation of Duties Matrix is as depicted in <Insert Appendix Letter>,"*** *and include a hyperlink to the appendix.*  *Delete this and all other instructional text from your final version of this document.* |

Table 11.1 <Insert CSO Name> Separation of Duties

| Duty Description | Information Owner | Security officer | Privacy officer | Linux Admin | Windows Admin | Agency Admin | Agency Customer |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Adds/Removes Privileged Admins | X | X |  |  |  |  |  |  |  |
| Adds/Removes Non-privileged Admins |  | X | X |  |  |  |  |  |  |
| Adds/Removes Customer Privileged Admins |  |  |  |  |  |  |  |  |  |
| Adds/Removes Customer Non-privileged Admins |  |  |  |  |  |  |  |  |  |
| Enforces Physical Access Authorizations |  |  |  |  |  |  |  |  |  |
| Defines Least Privilege Needed to Perform Tasks |  |  |  |  |  |  |  |  |  |
| Reviews/Approves Policy |  |  |  |  |  |  |  |  |  |
| Enforces Policy |  |  |  |  |  |  |  |  |  |

# SSP Appendices List

|  |
| --- |
| ***Instructions:*** |
| *FedRAMP provides templates for many of the required appendices. Some templates are available on FedRAMP’s* [Documents and Templates](https://www.fedramp.gov/documents-templates/) *Web page; others are included within the body of the SSP Appendix. Where FedRAMP provides a template, it will be noted in the table below (“FedRAMP-provided” versus “CSP-provided”).*  *Many of the appendices are not required for LI-SaaS CSOs. This is noted in the table below.*  *Add the file names, for each of the items below, except for those included within the SSP.*  *Additional appendices may be added to address additional content or to move tables from the front matter sections of the SSP. Be sure to add the appendix name and filename for any of the SSP tables that you opted to make into appendices. Be sure that all appendices are included with this SSP.*  *Delete this and all other instructional text from your final version of this document.* |

Table 12.1 SSP Required Appendices

| Appendix Name | Filename |
| --- | --- |
| **Appendix A: FedRAMP Security Controls**  (FedRAMP-provided; different template for each impact level) |  |
| **Appendix B: Related Acronyms**  (CSP-provided) | Included within the SSP |
| **Appendix C: Security Policies and Procedures**  (CSP-provided in a zip file; not required for LI-SaaS) |  |
| **Appendix D: User Guide**  (CSP-provided; not required for LI-SaaS) |  |
| **Appendix E: Digital Identity Worksheet**  (FedRAMP-provided) | Included within the SSP |
| **Appendix F: Rules of Behavior**  (FedRAMP-provided; not required for LI-SaaS) |  |
| **Appendix G: Information System Contingency Plan (ISCP)**  (FedRAMP-provided; not required for LI-SaaS) |  |
| **Appendix H: Configuration Management Plan (CMP)**  (CSP-provided; not required for LI-SaaS) |  |
| **Appendix I: Incident Response Plan (IRP)**  (CSP-provided; not required for LI-SaaS) |  |
| **Appendix J: CIS and CRM Workbook**  (FedRAMP-provided; different template for each impact level) |  |
| **Appendix K: FIPS 199 Worksheet**  (FedRAMP-provided) | Included within the SSP |
| **Appendix L: CSO-Specific Required Laws and Regulations**  (CSP-provided) |  |
| **Appendix M: Integrated Inventory Workbook**  (FedRAMP-provided) |  |
| **Appendix N: Continuous Monitoring Plan**  (CSP-provided) |  |
| **Appendix O: POA&M**  (FedRAMP-provided) |  |
| **Appendix P: Supply Chain Risk Management Plan (SCRMP)**  (CSP-provided) |  |
| **Appendix Q: Cryptographic Module Table**  (FedRAMP-provided) |  |

1. <Insert CSO Name> FedRAMP Security Controls

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).*  *Select the appropriate baseline template (LI–SaaS, Low, Moderate, or High), from the* [FedRAMP Documents and Templates webpage](https://www.fedramp.gov/documents-templates/), *and maintain the controls as a separate attachment to the SSP. For LI-SaaS packages, Appendix A uses a consolidated approach that is completed by both the CSP prior to an assessment, and an IA during an assessment. The LI-SaaS Appendix A includes three sections:*   * *Section 1: Documented and Assessed Controls* * *Section 2: FedRAMP LI-SaaS Assessment Results* * *Section 3: FedRAMP LI-SaaS [System Name] Attestation Statement*   *The controls tables describe the security controls as they are implemented for the system. For each control, it is important to describe how the control is implemented, and from where the control originates, so that it is clear whose responsibility it is to implement, manage, and monitor the control. General instructions related to control inheritance and applicability are provided in the paragraph below. CSPs are highly encouraged to reference the* [FedRAMP CSP Authorization Playbook, Volume II](https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook_Getting_Started_with_FedRAMP.pdf) *for detailed guidance (including “Dos and Don’ts”) on how to document security controls.*  *Control inheritance needs to be considered for each control – both from the perspective of a CSO inheriting controls from another CSO (e.g., a SaaS inheriting controls from an underlying IaaS/PaaS), and inheritability of controls from a CSO by its customers (agencies or other CSPs). Please see below for additional guidance related to control inheritance:*   * *Remember that “inheritance” can be claimed from* ***FedRAMP Authorized services only.*** *If the system or service is not FedRAMP Authorized, a CSP is fully responsible for the control.* * *For controls that are inherited from another CSO, ensure the “Inherited” box is selected, provide the name of the CSO that it is being inherited from, and describe the functionality that is being inherited in the control implementation description.*    + *Note that “-1” controls (AC-1, AU-1, SC-1, etc.) are not 100% inherited. The inheriting CSP must describe their functions to enable inheritance. In some cases, the role may be minimal.*   *For controls defined as fully inheritable by a customer (agencies or other CSPs):*   * *A CSP is responsible for ensuring its implementation meets federal/FedRAMP control requirements.* * *An IA is required to validate that inherited security features can be inherited.*   *For a control that can only be inherited under a specific use case:*   * *A CSP must describe this use case in the control narrative.* * *An IA must validate the control inheritability, as dictated by the use case.*   *For controls defined as a customer responsibility, the customer (i.e., the agency or leveraging CSP) is responsible for implementing, documenting, and testing the control.*  *For shared responsibility controls:*   * *Function(s) provided by the CSP must be clearly documented in the control narrative, specifying the CSP’s responsibilities AND the responsibilities provided, or configured, by the customer.* * *An IA is required to test a CSP’s responsibilities.*   *For all controls, if a CSP provides options for the customer in implementing a control, the CSP must make clear what options are compliant with federal policy (e.g., for authentication mechanisms that can be chosen by the customer, a CSP must make it very clear which mechanisms are compliant and non-compliant).*   * *A CSP is NOT responsible for testing a customer’s implementation of an inherited control.* * *A CSP is NOT responsible for testing customer-responsible controls.*   *When referencing policies and procedures, in control narratives, be sure to include the document title, date or version, and applicable section or paragraph numbers so that it is clear which document is being referred to and where, within the document, applicable details can be found.*  *All areas where a control applies in a system, whether to the operating system (OS) variant, software, etc., it must be documented in the control narrative. Technical controls should explain how that control is addressed for each component of the solution (e.g., where multiple platforms in the system are identified by the hardware and software inventory, each platform must be addressed; at a minimum, each inventory category (i.e., Software Application, Appliance, Windows, Linux, Cisco, etc.) has access controls, audit logging, session controls, etc., and each may have those controls configured uniquely for each component type. It is expected to have unique implementations addressed by platforms for the controls/control families AC, IA, AU, CM, SI, and SC, where applicable.*  *Delete this and all other instructional text from your final version of this document.* |

Please see Appendix A (separate document) for the security controls applicable to <Insert CSO Name>.

1. <Insert CSO Name> Related Acronyms

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).*  *Document CSO/CSP-specific acronyms in this appendix. They should also be spelled out, when first used, in the SSP. The format for this appendix is at the CSP’s discretion.*  *Delete this and all other instructional text from your final version of this document.* |

The acronyms that appear in this section are specific to the <Insert CSO Name> SSP.

1. <Insert CSO Name> Information Security Policies and Procedures

|  |
| --- |
| ***Instructions:*** |
| *This appendix is not required for LI-SaaS CSOs (see Appendix A LI-SaaS for attestation requirements).*  *Policies and procedures (P&Ps) are a critical supplement to the SSP and are required by the first control (known as the “dash ones” (e.g., AC-1)) for each control family. Policies provide the guidelines under which the accompanying procedures are developed and by which the SSP controls are implemented. Procedures define general instructions necessary to implement a control; for example:*  *“Based on the approved account request ticket, DevsOps will add the user to the in-boundary AD instance, and assign the user to the FedRAMP group as well as any other groups specified within the account request ticket.”*  *Procedures typically do not include command-level instructions that are found in internal standard operating procedures (SOPs).*  *FedRAMP does not provide templates for P&Ps. Some CSPs choose to combine all policies into a single document and all procedures into a single document. Some CSPs choose to develop separate P&Ps for each control family. Either approach is acceptable, as long as the requirements for each “dash one” control are satisfied, and the reviewer understands how to locate the P&Ps associated with each control family.*  *Be sure to upload the policy and procedure document(s) to your secure repository, ensuring accessibility by Agency users.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> policies and procedures are included in Appendix C, available separately.

1. <Insert CSO Name> User Guide

|  |
| --- |
| ***Instructions:*** |
| *Instructions: This appendix is not required for LI-SaaS CSOs.*  *The user guide explains how agency customers will use the system (e.g., if a system has a self-service portal, the user guide must explain how to use the portal).*  *FedRAMP does not provide a template for the User Guide. Many CSPs provide guidance and instructions to agency customers via a dynamic website versus a separate static document. This is perfectly acceptable. Be sure to note the website address below. If the information is not publicly accessible, include instructions for requesting access.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> user guide is included in Appendix D, available separately.

or

The <Insert CSO Name> user guide website address is <Insert CSO User Guide URL>.

1. <Insert CSO Name> Digital Identity Worksheet

|  |
| --- |
| ***Instruction:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).*  *Complete Table E.2, below; a separate attachment is not required. Authentication solutions, provided by a CSP for CSP-personnel to access and administer the CSO, must meet digital identity requirements. Authentication solutions provided by a CSP, for customers to access the CSO, must also meet digital identity requirements.*  *Delete this note and all other instructional text from your final version of this document.* |

**Mapping FedRAMP Levels to NIST SP 800-63 Levels**

Digital identity is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on the identity proofing process, the authenticator management process, and the assertion protocol used in a federated environment to communicate authentication and attribute information, if applicable.

Table E.1, below, “Mapping FedRAMP Levels to NIST SP 800-63 Levels”, maps the FedRAMP impact levels (Low/LI-SaaS, Moderate, and High) to [NIST SP 800-63 Digital Identity Guidelines](https://pages.nist.gov/800-63-3/) levels:

* Identity Assurance Level (IAL) - Refers to the identity proofing process
* Authenticator Assurance Level (AAL) - Refers to the authentication process
* Federation Assurance Level (FAL) - Refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable), to a relying party (RP)

Table E.1 Mapping FedRAMP Levels to NIST SP 800-63 Levels

| FedRAMP Impact Level | Identity Assurance Level (IAL) | Authenticator Assurance Level (AAL) | Federation Assurance Level (FAL) |
| --- | --- | --- | --- |
| **High** | IAL3: In-person or supervised remote identity proofing | AAL3: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography; authenticator must be hardware-based | FAL3: The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it. For very high value or very high-risk situations, the subscriber (user) must provide proof of possession of a secure, cryptographic key, and a HW based device to provide verifier impersonation resistance. The device may fulfill both requirements. |
| **Moderate** | IAL2: In-person or remote, potentially involving a “trusted referee” | AAL2: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography | FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Low and  FedRAMP LI-SaaS** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor; verifiers use FIPS 140-validated cryptography | FAL1: Assertion is digitally signed by the identity provider |

**Digital Identity Level Selection**

|  |
| --- |
| ***Instructions:*** |
| *Select the lowest level that will cover all potential impacts identified from the table above.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSP Name> has identified that they support the digital identity level that has been selected for the <Insert CSO Name>. The selected digital identity level indicated is supported for federal agency consumers of the CSO. Implementation details of the digital identity mechanisms are provided in Appendix A under control IA-2.

Table E.2 Digital Identity Level

| Digital Identity Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: AAL1, IAL1, FAL1 | Low/LI-SaaS |  |
| Level 2: AAL2, IAL2, FAL2 | Moderate |  |
| Level 3: AAL3, IAL3, FAL3 | High |  |

1. <Insert CSO Name> Rules of Behavior (RoB)

|  |
| --- |
| ***Instructions:*** |
| *This appendix is not required for LI-SaaS CSOs.*  *Security control PL-4 requires CSPs to develop Rules of Behavior (RoB) that establish and describe the responsibilities and expected behavior related to the use of a CSO.*  *FedRAMP provides a* [*RoB template*](https://www.fedramp.gov/assets/resources/templates/SSP-A05-FedRAMP-RoB-Template.docx) *that includes four example sets of rules of behavior: two for internal users (privileged and non-privileged) and two for external users (privileged and non-privileged). CSPs should tailor these rule sets, as appropriate, to define the rules of behavior necessary to secure a CSO.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> rules of behavior are included in Appendix F, attached separately.

1. <Insert CSO Name> Information System Contingency Plan (ISCP)

|  |
| --- |
| ***Instructions:*** |
| *This appendix is not required for LI-SaaS CSOs.*  *FedRAMP provides an* [Information System Contingency Plan (ISCP) template](https://www.fedramp.gov/assets/resources/templates/SSP-A06-FedRAMP-ISCP-Template.docx) *that must be used by a CSP.*  *A CSP is responsible for establishing general procedures for recovering their CSO after a service disruption. Security control CP-2 requires CSPs to develop a contingency plan for their CSO. The ISCP establishes comprehensive procedures to recover a CSO quickly and effectively following a service disruption.*  *Keystroke-level procedures are not commonly included in the ISCP. These procedures are typically considered system sensitive and are only shared when required for audits and assessments.*  *TIP: A business impact analysis (BIA) is required as Appendix M of the ISCP. FedRAMP does not provide a BIA template; however,* [NIST SP 800-34, Contingency Planning Guide for Federal Information Systems](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final), *includes a sample BIA template, in Appendix B.*  *NOTE: Security control CP-4 requires CSPs to test the ISCP, at least annually, and document the results in a test report as well as coordinate the review and approvals of test plans (prior to execution) and test results. The test report must be included in the ISCP. CSPs must conduct a test of the ISCP prior to achieving a FedRAMP authorization and at least annually, thereafter, as part of continuous monitoring.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> information system contingency plan is included in Appendix G, attached separately.

1. <Insert CSO Name> Configuration Management Plan (CMP)

|  |
| --- |
| ***Instructions:*** |
| *This appendix is not required for LI-SaaS CSOs.*  *Security control CM-9 requires CSPs to develop a CMP, in accordance with NIST SP 800-128. FedRAMP does not provide a template for the CMP; however,* [NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems](https://csrc.nist.gov/publications/detail/sp/800-128/final), *provides guidelines for the implementation of CM controls as well as a sample CMP outline in Appendix D.*  Delete this and all other instructional text from your final version of this document. |

The <Insert CSO Name> configuration management plan is included as Appendix H, attached separately.

1. <Insert CSO Name> Incident Response Plan (IRP)

|  |
| --- |
| ***Instructions:*** |
| *This appendix is not required for LI-SaaS CSOs.*  *Security control IR-8 requires CSPs to develop an IRP, in accordance with NIST SP 800-61. FedRAMP does not provide an IRP template; however,* [NIST SP 800-61, Computer Security Incident Handling Guide](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)*, provides guidance on the development of incident response policies and procedures as well as guidance on the development of an IRP.*  *TIP: When developing an IRP, be sure to incorporate the incident reporting requirements defined in the* [FedRAMP Incident Communications Procedures](https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf)*. This document outlines the steps for FedRAMP stakeholders to use when reporting information concerning information security incidents, including responses to published emergency directives.*  *NOTE: Security control IR-3 requires CSPs to test an IRP, at least annually, and document the results as well as coordinate the review and approvals of test plans (prior to execution) and test results. Some CSPs incorrectly assume that this requirement only applies during ongoing continuous monitoring (post-authorization). CSPs must conduct a test of the IRP prior to achieving a FedRAMP authorization, and at least annually, thereafter, as part of continuous monitoring.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> incident response plan is included as Appendix I, attached separately.

1. <Insert CSO Name> Control Implementation Summary (CIS) and Customer Responsibilities Matrix (CRM) Workbook

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).*  *CSPs are required to submit a single control implementation summary (CIS) and customer responsibilities Matrix (CRM) workbook as Appendix J to the SSP. FedRAMP provides one template with color-coded tabs (worksheets) for each of the four FedRAMP baselines (LI-SaaS, Low, Moderate, and High). The FedRAMP CIS and CRM Workbook is available on the* [FedRAMP Templates website](https://www.fedramp.gov/templates/).  *There is a single Instructions tab included in the FedRAMP CIS and CRM Workbook that provides guidance for completing the CIS and CRM.*  *The “CIS” tab, for each baseline type, provides a summary of the implementation status (Implemented, Partially Implemented, Planned, Alternative Implementation, or N/A) of the security controls applicable to a CSO. It also identifies the control origination (i.e., the responsible party or parties) for each of the controls.*  *The “CRM” tab, for each baseline type, describes the specific elements of each control where the responsibility lies with the customer. There are examples provided, as a separate tab, that apply to the LI-SaaS, Low, Moderate, and High baselines. This must be done for any control with a control origination of:*   * *Configured by Customer (Customer System Specific)* * *Provided by Customer (Customer System Specific)* * *Shared (Service Provider and Customer Responsibility)*   *TIP: Agencies rely on the CIS and CRM Workbook to understand the scope and nature of customer-specific responsibilities. Often, it is the first document opened by the AO (or designee) when reviewing an authorization package. For this reason, it is critically important to ensure that the information in the workbook is accurate and* ***consistent with the SSP****. Before submitting the authorization package, set aside time to conduct a crosswalk between the SSP and CIS and CRM Workbook. This will go a long way towards preventing delays during the review process.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> CIS and CRM workbook is included as Appendix J, attached separately.

1. <Insert CSO Name> Federal Information Processing Standard (FIPS) 199 Categorization

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).*  *Review the* [NIST Special Publication 800-60 Volume 2 Revision 1](https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final)*,“Appendix C: Management and Support Information and Information System Impact Levels,” and “Appendix D: Impact Determination for Mission-Based Information and Information Systems” to assess the recommended impact level for each of the information types. For more information, consult Appendix D.2.*  *After reviewing the NIST guidance on information types, complete Table K.1, CSP Applicable Information Types with security impact levels using NIST SP 800-60 V2 R1. In the first three columns of the table, specify the NIST SP 800-60 V2 R1 recommended impact level. In the next three columns, specify the CSP-determined recommended impact level. If the CSP-determined recommended impact level does not match the level recommended by NIST, add an explanation in the last column as to why this decision was made.*  *The FIPS level, determined in Table K.1, should also be recorded in Section 3, Table 3.1, System Information, of this SSP.*  *Instructions for LI-SaaS only: The only personally identifiable information (PII) allowed in the system is the minimum necessary to provide login information. To be considered a FedRAMP LI-SaaS cloud service, the answer to all 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](https://csrc.nist.gov/publications/detail/sp/800-145/final)*?* 4. *Does the cloud service contain no 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](https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf)*?* 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?*   *Delete this and all other instructional text from your final version of this document.* |

The FIPS 199 Categorization (Security Categorization) report is a key component of the security authorization package developed for submission to FedRAMP authorizing officials. The FIPS 199 Categorization report below includes the determination of the security impact level for the <Insert CSO Name> cloud environment.

Note: This report is initially completed by the CSP in anticipation of what the actual federal data that might be stored, processed, and transmitted. Each agency must do this FIPS 199 analysis for their own data flows to ensure compatibility with the overall criticality level.

The <Insert CSO Name> system has been determined to have a security categorization of <Insert CSO Security Categorization Level>, as determined in Table K.1.

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS 199 is the High watermark for the impact level of all the applicable information types.

Table K.1 uses the NIST SP 800-60 (current revision) Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table K.1 <Insert CSO Name> Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

| Information Type | NIST SP 800-60 V2 R1  Recommended Confidentiality Impact Level | NIST SP 800-60 V2 R1  Recommended Integrity Impact Level | NIST SP 800-60 V2 R1  Recommended Availability Impact Level | CSP Selected Confidentiality Impact Level | CSP Selected Integrity Impact Level | CSP Selected Availability Impact Level | Statement for Impact Adjustment Justification |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. <Insert CSO Name>-Specific Laws and Regulations

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High)*  *If the CSO is governed by CSP or agency-specific laws and regulations, these should be listed below. If there are no CSO-specific governing laws or regulations, simply state “N/A” in the table.*  *Delete this and all other instructional text from your final version of this document.* |

Table L.1 <Insert CSO Name>-specific Laws and Regulations

| **Number** | **Title** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

1. <Insert CSO Name> Integrated Inventory Workbook (IIW)

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).*  *Security control CM-8 requires CSPs to develop and document an inventory of system components within the authorization boundary that is at the level of granularity deemed necessary for tracking and reporting. To this end, FedRAMP provides an* [Integrated Inventory Workbook (IIW) Template](https://www.fedramp.gov/assets/resources/templates/SSP-A13-FedRAMP-Integrated-Inventory-Workbook-Template.xlsx) *that CSPs must complete and submit as Appendix M of the SSP. Instructions for completing the IIW are provided in the template.*  *Consistency is key to providing a good SSP. The inventory should be consistent with what is depicted in the SSP diagrams. SSP reviewers should not have any issues identifying the key inventory components, as these are represented in the SSP diagram.*  *CSPs are also required to update the IIW as part of* ***monthly*** *continuous monitoring efforts.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> integrated inventory workbook is included in Appendix M, attached separately.

1. <Insert CSO Name> Continuous Monitoring Plan

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High). FedRAMP does not provide a template for the continuous monitoring plan. CSPs should use their own desired format to develop a continuous monitoring plan, in accordance with CA-7. The* [FedRAMP Continuous Monitoring Strategy Guide](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj_hMGu_uf6AhW2FFkFHXxPBhkQFnoECA4QAQ&url=https%3A%2F%2Fwww.fedramp.gov%2Fassets%2Fresources%2Fdocuments%2FCSP_Continuous_Monitoring_Strategy_Guide.pdf&usg=AOvVaw1qjKxngLGTjnAXLIr1IYg1) *provides guidance and instructions on how to implement a continuous monitoring program, and the guidance may be used to help formulate a continuous monitoring plan.*  *Additionally, CSPs must use the FedRAMP-provided* [FedRAMP Continuous Monitoring Monthly Executive Summary](https://www.fedramp.gov/assets/resources/templates/FedRAMP-Continuous-Monitoring-Monthly-Executive-Summary-Template.xlsx) *that is submitted with the initial authorization package and updated as part of continuous monitoring. Updates should be uploaded in the CSO’s FedRAMP Secure Repository continuous monitoring subdirectory.*  *Delete this and all other instructional text from your final version of this document.* |

The <CSO Name> continuous monitoring plan is included in Appendix N, attached separately.

1. <Insert CSO Name> POA&M

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High), and CSPs must use the* [FedRAMP-provided POA&M template](https://www.fedramp.gov/assets/resources/templates/FedRAMP-POAM-Template.xlsm).  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> plan of action and milestones (POA&M) is included in Appendix O, attached separately.

1. <Insert CSO Name> Supply Chain Risk Management Plan (SCRMP)

|  |
| --- |
| ***Instructions:*** |
| *This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High). FedRAMP does not provide a template for the supply chain risk management plan. CSPs should use their own desired format to develop this plan, in accordance with SR-2. A plan format is available, for reference, in NIST SP 800-161 (current revision).*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> supply chain risk management plan (SCRM) is included in Appendix P, attached separately.

1. <Insert CSO Name> Cryptographic Modules Table

|  |
| --- |
| ***Instructions:*** |
| *Instructions: This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High) and, CSPs must use the* [FedRAMP provided Cryptographic Modules Table template](https://fedramp.gov/assets/resources/templates/SSP-Appendix-Q-Cryptographic-Modules-Table.docx).  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> cryptographic modules table is included as Appendix Q, attached separately.