Logo

Description automatically generated

info@fedramp.gov

fedramp.gov

FedRAMP® Moderate Readiness Assessment Report (RAR) Template

**for <Insert CSP Name>**

**<Insert CSO Name>**

<Version X.X>

<MM/DD/YYYY>

**Company Sensitive and Proprietary  
For Authorized Use Only**

|  |
| --- |
| **IMPORTANT:** This FedRAMP Readiness Assessment Report (RAR) template is intended for systems categorized at the **Moderate** security impact level, in accordance with the Federal Information Processing Standards (FIPS) Publication 199 security categorization. A RAR template for High systems is available on the FedRAMP website.  Cloud service providers (CSPs) may also use the RAR template to do a self-assessment, prior to engaging with a FedRAMP recognized third party assessment organization (3PAO).  **FedRAMP Ready status is valid for one calendar year after designation from the FedRAMP Program Management Office (PMO).** |

# THIRD PARTY ASSESSMENT ORGANIZATION (3PAO) ATTESTATION

|  |
| --- |
| ***Instructions:*** |
| *A FedRAMP recognized 3PAO must attest to the readiness of the CSP’s system. To be considered FedRAMP Ready, the CSP must meet all the requirements in Section 4.1, Federal Mandates. In addition, the 3PAO must assess the CSP’s ability to meet the requirements in Section 4.2, FedRAMP Requirements. The 3PAO must use its expert judgment to subjectively evaluate the CSP’s overall readiness and factor this evaluation into their attestation.*  ***THE 3PAO SHOULD SUBMIT THE RAR ONLY IF THE 3PAO HAS FULLY VALIDATED (1) THE CSO AUTHORIZATION BOUNDARY AND DATA FLOW DIAGRAMS, (2) THE CSP HAS IMPLEMENTED ALL FEDERAL MANDATES, and (3) THERE ARE NO MAJOR TECHNICAL GAPS BETWEEN THE CSP’S IMPLEMENTED TECHNICAL CONTROLS AND FEDRAMP REQUIREMENTS.***  *The FedRAMP Director will make a determination, based on the RAR, whether the cloud service offering (CSO) is suitable for a FedRAMP authorization. The FedRAMP Director will provide a letter to the CSP that outlines the results of the review.*  *Before delivering the final version of the RAR, be sure to delete all italicized instructional text.*  Delete instruction text after completion. |

|  |
| --- |
| [3PAO name] attests to the accuracy of the information provided in this FedRAMP Readiness Assessment Report (RAR) and the [CSP name and CSO name]’s readiness to meet the FedRAMP requirements as described in this RAR. [3PAO name] recommends that the FedRAMP PMO grant [CSO name] “FedRAMP Ready” status, based on the CSP’s security capabilities as of [Assessment Completion Date].  This attestation is based on [3PAO name]’s 3PAO accreditation by the American Association for Laboratory Accreditation (A2LA), FedRAMP recognition, experience and knowledge of the FedRAMP requirements, and knowledge of industry cybersecurity best practices.  This FedRAMP RAR was created in alignment with FedRAMP requirements and guidance. While this report only contains summary information regarding a CSP’s ability to meet the FedRAMP requirements, it is based on [3PAO name]’s active validation of [CSP name and CSO name]’s security capabilities through observations, evidence reviews, personnel interviews, and demonstrated capabilities of security implementations. This FedRAMP RAR is valid for one calendar year after designation from the FedRAMP PMO.  Lead Assessor’s Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <Lead Assessor’s Name>  <3PAO Name> |

# READINESS ASSESSMENT INFORMATION

|  |
| --- |
| ***Instructions:*** |
| *Provide and validate the information below. This RAR template is intended for systems categorized at the* ***Moderate*** *security impact level, in accordance with the FIPS Publication 199 security categorization.*  Delete instruction text after completion. |

*Table 0-1. System Information*

|  |  |
| --- | --- |
| System Information | |
| **CSP Name:** |  |
| **CSO Name (and Abbreviation):** |  |
| **FedRAMP Unique Identifier:** |  |
| **Service Model:** | (IaaS, PaaS, SaaS) |
| **FIPS PUB 199 System Security Level: (Moderate)** |  |
| **Digital Identity Determination Level:** | (IAL2/FAL2/AAL2, IAL3/FAL3/AAL3) |
| **Fully Operational\* as of:** | Enter the date the system became fully operational. |
| **Number of Customers (US Federal/Others):** | Enter # of US Federal customers / # of other customers. |
| **Deployment Model:** | Public Cloud, Government-Only Cloud, Hybrid Cloud |
| **System Functionality:** | Briefly describe the functionality of the system and service being provided. |

*\*Fully Operational means that the architectural components of the system are all in place and operating as required, and the technical controls are implemented. However, for a RAR, the documentation may be partially developed.*

# 

TEMPLATE REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Template Version** | **Author** |
| 04/26/2017 | Initial release version | 1.0 | FedRAMP PMO |
| 08/28/2018 | Added clarifications throughout. Added requirements that provide better visibility into system interconnections and external services. | 1.1 | FedRAMP PMO |
| 02/13/2019 | Verbiage added to the top of the document and to the 3PAO attestation stating the expiration date of the report. | 1.2 | FedRAMP PMO |
| 07/31/2020 | Updated to include Locality checks for data centers | 1.3 | FedRAMP PMO |
| 04/1/2021 | Updated Table 4-3 Transport Layer Security to include TLS 1.3 | 1.4 | FedRAMP PMO |
| 01/4/2022 | Added clarifications throughout. Updated to clarify requirements that apply to CSPs pursuing a JAB P-ATO but do not apply to an Agency ATO. Rearranged sections to reduce duplicate information and improve document flow. Updated instructional notes. | 1.5 | FedRAMP PMO |
| 06/30/2023 | Updated to reflect FedRAMP Rev. 5 baselines. Added 3PAO validation of DNSSEC responses. | 2.0 | FedRAMP PMO |
| 5/31/2024 | Rewrote the instructions for Section 4.2.1 - Approved Cryptographic Modules [SC-13]. Removed an outdated statement, related to HTTPS Strict Transport Security (HSTS), in Section 4.2.2 - Transport Layer Security. Removed outdated JAB references throughout the document. | 2.1 | FedRAMP |

TABLE OF CONTENTS

[THIRD PARTY ASSESSMENT ORGANIZATION (3PAO) ATTESTATION 1](#_Toc167844169)

[READINESS ASSESSMENT INFORMATION 2](#_Toc167844170)

[1. Introduction 7](#_Toc167844171)

[1.1. Purpose 7](#_Toc167844172)

[1.2. Outcomes 7](#_Toc167844173)

[1.3. FedRAMP Approach and Use of This Document 8](#_Toc167844174)

[2. General Guidance and Instructions 9](#_Toc167844175)

[2.1. Embedded Document Guidance 9](#_Toc167844176)

[2.2. Additional Instructions to 3PAOs 9](#_Toc167844177)

[3. System Information 11](#_Toc167844178)

[3.1. Authorization Boundary 11](#_Toc167844179)

[3.2. Leveraged FedRAMP Authorizations 14](#_Toc167844180)

[3.3. External & Corporate Systems and Services 15](#_Toc167844181)

[3.4. APIs 11](#_Toc167844182)

[3.5. Trusted Internet Connection (TIC) [SC-7(3)] 13](#_Toc167844183)

[3.6. Data Flow Diagrams 13](#_Toc167844184)

[3.7. Separation Measures [AC-2, AC-4, SC-7] 14](#_Toc167844185)

[4. Capability Readiness 15](#_Toc167844186)

[4.1. Federal Mandates 15](#_Toc167844187)

[4.2. FedRAMP Requirements 16](#_Toc167844188)

[4.2.1. Approved Cryptographic Modules [SC-13] 16](#_Toc167844189)

[4.2.2. Transport Layer Security [NIST SP 800-52, most current revision] 17](#_Toc167844190)

[4.2.3. Identification, Authentication, and Access Control 18](#_Toc167844191)

[4.2.4. Audit, Alerting, Malware, and Incident Response 19](#_Toc167844192)

[4.2.5. Contingency Planning and Disaster Recovery 21](#_Toc167844193)

[4.2.6. Configuration and Risk Management 23](#_Toc167844194)

[4.2.7. Data Center Security 25](#_Toc167844195)

[4.2.8. Policies, Procedures, and Training 26](#_Toc167844196)

[4.3. Additional Capability Information 26](#_Toc167844197)

[4.3.1. Change Management Maturity 27](#_Toc167844198)

[4.3.2. Continuous Monitoring (ConMon) Capabilities 27](#_Toc167844199)

[4.3.3. Status of System Security Plan (SSP) 29](#_Toc167844200)

1. Introduction

Purpose

This report and its underlying assessment are intended to enable FedRAMP to reach a FedRAMP Ready decision for a specific CSP’s offering, based on organizational processes and the security capabilities of the Moderate-impact information system. FedRAMP grants a FedRAMP Ready designation when the information in this report indicates the CSP is likely to achieve a FedRAMP authorization for the offering.

It is important that the overall alignment with the National Institute of Standards and Technology (NIST) definition of cloud computing according to NIST SP 800-145 are met (NOTE: This includes the requirement for the CSP to have a self-service portal). This report will also identify notable strengths and weaknesses; ability to consistently maintain a clearly defined system boundary; ability to accurately describe intra and inter-system user and sensitive metadata data flow; risks associated with interconnections used to transmit federal data/metadata or sensitive system data/metadata; and risks associated with the use of external systems and services that are not FedRAMP Authorized.

In addition, this report will clearly define customer responsibilities and outline unique or alternative implementations. It will highlight overall maturity level relative to the system type, size and complexity along with overall operational maturity relative to how long the system and required security controls have been in operation.

Outcomes

A 3PAO should only submit this report to FedRAMP if it determines the CSP’s system is fully ready to pursue, and likely to achieve, a FedRAMP authorization at the Moderate security impact level within one (1) year from the date of submission.

Submission of this report by the 3PAO does not guarantee a FedRAMP Ready designation, nor does it guarantee a FedRAMP authorization.

During the RAR review and approval process, the FedRAMP PMO may require the CSP to perform additional actions to demonstrate readiness, which would require validation by the 3PAO. Concurrently, the FedRAMP PMO may require updates to provide clarity.

3PAOs conducting Readiness Assessments should advise CSPs that additional changes may be required after the RAR is submitted to the FedRAMP PMO for review and approval.

The FedRAMP Director will make a determination, based on the RAR, if the CSO is suitable for FedRAMP authorization.

FedRAMP Approach and Use of This Document

The RAR identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of subjective information. The clear and objective requirements enable the 3PAO to concisely identify whether a CSP is achieving the most important FedRAMP Moderate baseline requirements. The combination of objective requirements and subjective information enables FedRAMP to render a readiness decision based on a more complete understanding of the CSP’s ***current*** security capabilities.

Section 4, Capability Readiness, is organized into three sections:

* **Section 4.1, Federal Mandates**, identifies a small set of the federal mandates a CSP must satisfy. FedRAMP will not waive any of these requirements.
* **Section 4.2, FedRAMP Requirements,** identifies an excerpt of the most compelling requirements from the NIST Special Publication (SP) 800 document series and FedRAMP guidance. A CSP is unlikely to achieve a FedRAMP authorization if any of these requirements are not met.
* **Section 4.3, Additional Capability Information,** identifies additional information, not tied to specific requirements, that has typically reflected strongly on a CSP’s ability to achieve a FedRAMP authorization.

1. General Guidance and Instructions

Embedded Document Guidance

This document contains embedded text intended to instruct the 3PAO on how to complete each section. These instructions ensure FedRAMP receives all the information necessary to render a FedRAMP Ready decision.

|  |
| --- |
| ***Instructions:*** |
| Before delivering the final version of the RAR, be sure to delete all italicized instructional text.  Delete instruction text after completion. |

Additional Instructions to 3PAOs

3PAOs must adhere to the following instructions when preparing the RAR:

1. Do NOT submit the completed Moderate RAR without first coordinating with the FedRAMP PMO via info@fedramp.gov.
2. On the Title Page, enter the CSP name, CSO name, version number, and date of this RAR submission. If this is a re-submission, be sure to increment the version number and adjust the date.
3. The RAR must provide:
   1. An overview of the system;
   2. A subjective summary of the CSP’s overall readiness, including rationale such as notable strengths and other areas for consideration;
   3. An assessment of the CSP’s ability to meet the federal mandates identified in Section 4.1, the FedRAMP requirements identified in Section 4.2, and additional capabilities identified in Section 4.3;
   4. A clear description and diagram of system components and services, within the authorization boundary, as well as all connections to external systems and services that are outside of the authorization boundary;
   5. A clear Data Flow diagram(s) and description(s) that accounts for all intra and inter-boundary flow of federal information, data, and metadata. This includes all flows through the authorization boundary and to/from external systems and services and all flows between systems within the authorization boundary; and
   6. The 3PAO’s attestation regarding the CSP’s readiness to meet FedRAMP Moderate baseline requirements within one (1) year from the date of submission.
4. FedRAMP will not consider a CSP for a FedRAMP Ready designation unless all the requirements in Section 4.1, Federal Mandates, are met. 3PAOs should not recommend FedRAMP Ready status for CSPs that have not met ***all*** federal mandates (Note: Meeting these requirements does not guarantee a FedRAMP Ready designation).
5. 3PAOs must assess the system's technical, management, and operational capabilities using a combination of methods, including interview, observation, demonstration, examination, and onsite visits (e.g., in-person interviews and data center visits, as needed). 3PAOs may use CSP-provided diagrams, but must validate the diagrams as though the 3PAO created them. 3PAOs must not conduct this Readiness Assessment exclusively by reviewing a CSP's written documentation and performing interviews alone. **Active validation of all information provided within this report is required.**
6. 3PAOs must complete all sections and address **all elements of each question.** 3PAOs must also describe observations of any missing elements (e.g., if the CSP fails to meet all of the question elements). If a capability is fully inherited, answer "yes" and write "fully inherited" in the column provided for the capability description.
7. Control references are provided with each of the questions in Section 4.2, FedRAMP Requirements. These references are provided to help the 3PAO understand the basis for each question; however, the 3PAO is expected to consider all relevant FedRAMP security controls and capabilities when assessing the CSP's capabilities.
8. FedRAMP believes a typical level of effort for conducting a Readiness Assessment for mid-size, straightforward systems is between two (2) and four (4) weeks, with the first half focused on information gathering and the second half focused on analysis and report development.
9. System Information

Authorization Boundary

|  |
| --- |
| **IMPORTANT:** Ensuring authorization boundary accuracy in the RAR is critical to FedRAMP authorization activities. Inaccuracies within the RAR may give authorizing officials and FedRAMP grounds for removing a CSP from assessment and authorization activities. |

An authorization boundary provides a diagrammatic illustration of a CSO’s internal services, components, and other devices, along with connections to external services and systems. Please note that external services include external cloud services that are not FedRAMP Authorized, corporate shared services, and the external entities to which the system must connect to receive updates for products installed within the system boundary.

An authorization boundary accounts for all federal information, data, and metadata that flow through a CSO. If the CSO has strong configuration management and change management built into the system development life cycle, the development environment can be outside the CSO boundary. This means that there is a 3PAO validated, reproducible and effective way to make service changes without impacting the production environment.

|  |
| --- |
| **IMPORTANT:** Under most circumstances, the FedRAMP PMO has concern when a Moderate service leverages any systems that are not FedRAMP Authorized at the same impact level.  All external systems or services, used by a CSO, should be reviewed including their impact level and authorization type and data types being processed, stored, or transmitted to the external system or service. 3PAOs should identify potential risk to the CSO using the guidance and instructions in Sections 3.3 and 3.4. |

|  |
| --- |
| ***Instructions:*** |
| The 3PAO must perform full authorization boundary validation for the RAR, ensure nothing is missing from the CSP-identified boundary, and ensure all included items are currently present and are part of the system inventory. To achieve this, the 3PAO must perform activities including, but not limited to, discovery scans, in-person interviews, and physical examinations where appropriate. 3PAOs should use the [FedRAMP Authorization Boundary](https://www.fedramp.gov/assets/resources/documents/CSP_A_FedRAMP_Authorization_Boundary_Guidance.pdf) guidance as a reference when assessing and validating the authorization boundary.  Delete instruction text after completion. |

|  |
| --- |
| ***Instructions:*** |
| Insert 3PAO-validated network and architecture diagram(s) and provide a written description of the authorization boundary. The 3PAO must ensure the diagram:   * *Provides an easy to read, high resolution diagram that includes a legend.*   + *It is acceptable to provide the ABD as a separate attachment.* * *Includes a prominent RED border drawn around all components in the authorization boundary.* * *Depicts all ingress/egress points.* * *Depicts services leveraged from the underlying IaaS/PaaS and identifies any services that are not FedRAMP Authorized.*   + *How you do this is up to you; some CSPs use color-coding with a corresponding legend. Others have included a call-out box that lists all services that are not FedRAMP Authorized.* * *Depicts all interconnected systems and external services, including corporate shared services, and identifies any systems/services that are not FedRAMP Authorized.* * *Depicts every tool, service, or component that is mentioned in the SSP narrative and controls.*   + *This includes services used to manage and operate the system (e.g., security information and event management (SIEM), vulnerability scanning, system health monitoring, and ticketing).*   + *Identify all depicted tools, services, or components as either external or internal to the boundary.* * *Depicts how CSP admins and agency customers access the cloud service (i.e., authentication used to access service). While you will cover these in detail in the data flow diagrams, FedRAMP requires this information on the boundary diagram.* * *If applicable, depicts components provided by the CSP, and installed on customer devices, as inside the authorization boundary.*   + *These components are required to be in the boundary if they materially affect the CIA of the CSO or are essential for the customer’s use of the service (e.g., data collectors in customer data centers and mobile applications).* * *Shows connections between components within the boundary and to/from external services.*   + *Examples include connections from load balancers to the servers they support. Similar flows can be combined or noted (e.g., bastion server access to all hosts, all devices forward logs to log server, etc.)* * *Depicts development/test environment, alternate processing site, and location of backups.*   + *The development/test environment must be included within the boundary if federal data is used and/or if federal government personnel have access to the environment for any reason, including training and user acceptance testing.* * *Shows update services (e.g., malware signatures and OS updates) outside the boundary.* * *For the networking components of the diagram, ensure that the subnetworks and the locations of the DNSSEC authoritative and recursive name servers are illustrated.*   + *Ensure that the domain name(s) that is/are used for the USG instance of the CSO is/are illustrated on the diagram.*   Delete instruction text after completion. |

***NOTE:*** *The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand. If necessary, adjust the page orientation to landscape and/or use multiple diagrams to provide the best representation of the authorization boundary. If opting to use multiple diagrams, they must clearly correspond from one to another. We suggest a “parent and child” diagram structure to ensure clarity. Or the CSP may choose to create a larger area by using a larger layout size page and embedding this in the RAR. The embedded document must be easy to read and have a high resolution. The 3PAO must validate the content of the diagrams and narratives for accuracy for inclusion in the RAR and must make it clear in the RAR what (if any) content is CSP-supplied.*

Leveraged FedRAMP Authorizations

|  |
| --- |
| ***Instructions:*** |
| *If this Moderate system leverages another FedRAMP Authorized CSO (e.g., an IaaS that provides compute, network, and storage; or a SaaS that provides operational support services), provide the relevant details in Table 3-1 below. Please note:*   * *The CSO must be listed on the FedRAMP Marketplace with a status of “Authorized”.* * *3PAOs must validate that all sub-services listed in Table 3-1 are included in the leveraged CSO’s authorization boundary (refer to the CSO Service Description on the FedRAMP Marketplace). Services that are not included in a FedRAMP Authorized boundary must be listed in Table 3-3.* * *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 the 3PAO.* * *The Nature of Agreement can be any type of agreement between the CSP and the CSP vendors who support products (e.g., end-user license agreement (EULA), service level agreement (SLA), application license agreement, contract, etc.)* * Still Supported? Y or N - FedRAMP expects that all vendor products are kept current and patched.   Delete instruction text after completion. |

|  |
| --- |
| **IMPORTANT:** If there is a leveraged CSO, be sure to note every capability, in Section 4, that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability. |

*Table 3-1. Leveraged FedRAMP Authorizations*

| # | CSP and CSO Name | CSO Service | Authorization Type & FedRAMP Package ID | Nature of Agreement | Still Supported? Y or N |
| --- | --- | --- | --- | --- | --- |
| 1 | *Provide the names of the leveraged CSP and CSO (i.e., CSO name).* | *Describe the features and services/subservices provided by the CSO.* | *Provide the CSO’s FedRAMP Package ID.* |  |  |

External & Corporate Systems and Services

CSPs often establish connections to external systems and services to (i) exchange data and information or (ii) augment system functionality and operational support services. This includes corporate systems and services that are not part of the authorization boundary***. FedRAMP does not consider cloud systems and services as corporate systems and services*.** This means that if a corporate system and/or service is a cloud system within the corporate environment, that cloud system is considered an external service and must be designated as such.

|  |
| --- |
| ***Instructions:*** |
| *3PAOs must identify all connections to external systems and services in Table 3-2. The 3PAO should not include the leveraged services listed in Table 3-1. 3PAOs should not rely solely on CSP-provided boundary diagrams or interviews, but should use a combination of methods, such as analyzing data flows and ingress/egress rules, reviewing all open ports and service accounts, and examining solutions used to manage and operate the system. Connections to all external systems and services should also be depicted on the authorization boundary diagram in Section 3.1*.  Delete instruction text after completion. |

***NOTE:*** *FedRAMP defines a* ***connection*** *as any communication path used to push, pull, or exchange data and/or information, including application programming interfaces (APIs). For example, 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. 3PAOs must identify all API sets in Section 3.4, Table 3-3.*

*Table 3-2. External Systems and Services*

| # | System/Service Name | Interconnection Details | Nature of Agreement | Still Supported? Y or N | Data Types | Data Categorization | Authorized Users & Authentication Method | Compliance Programs |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***1*** | *Provide the name of the system or service. Include the vendor name, if different from the system or service name.* | *Provide connectivity details.* |  |  | *List the CSO data types transmitted to, stored, or processed by the system/service, including federal data/metadata and system data/metadata.* | *Identify the security impact level of the data (Low, Moderate, or High) in accordance with FIPS 199.* | *List the user roles (e.g., SecOps Engineers) authorized to access the service, and provide the authentication method.* | *List any certifications for this service (e.g., PCI SOC 2, CSA STAR Level 2), and provide the certification date.* |
|  | ***Description:*** *Describe the purpose of the external system/service and 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 customer data if the confidentiality, integrity, or availability (CIA) of the system/service were compromised. Please note: 3PAOs should carefully consider impact levels associated with metadata and the risk to the CSO or customer data if the CIA of the metadata were compromised. Describe any mitigations or compensating controls in place to reduce risk.*  ***Agreements:*** *Indicate whether an Interconnection Security Agreement (ISA), SLA, or other contractual agreement exists for this system/service.* | | | | | | | |
| ***2*** | *Service Name* | *Interconnection Details* |  |  | *Data Types* | *Data Categorization* | *Authorized Users & Authentication Method* | *Compliance Programs* |
|  | ***Description:***  ***Risk/Impact/Mitigation:***  ***Agreements:*** | | | | | | | |
| ***3*** | *Service Name* | *Interconnection Details* |  |  | *Data Types* | *Data Categorization* | *Authorized Users & Authentication Method* | *Compliance Programs* |
|  | ***Description:***  ***Risk/Impact/Mitigation:***  ***Agreements:*** | | | | | | | |

APIs

CSPs leverage public or custom APIs for all types of categories in computing. CSPs may use publicly available API sets provided by vendors or may develop custom APIs. APIs are categorized by functions such as backup and recover or communications.

If possible, 3PAOs should request the WSDL file for SOAP APIs and OpenAPI spec for REST APIs.

|  |
| --- |
| ***Instructions:*** |
| *Examples of public API sets are provided in Table 3-3 and the URL below. 3PAOs must identify all public or custom CSP-leveraged API sets that allow data to flow to and from the system. Remove the examples and use the blank rows in Table 3-3 to enter the API sets. Add new rows as needed. Optionally, embed a separate Excel spreadsheet if the list is too extensive.*  Delete instruction text after completion. |

*Table 3-3. APIs*

| API/CLI | Protocol | Authentication | Encryption Algorithm(s) | Data Types | Data Categorization | Description |
| --- | --- | --- | --- | --- | --- | --- |
| *CSO A API* | *TCP/NN* | *API Key* | *Encryption algorithms allowed* | *List the CSO data types transmitted to, stored, or processed by the system/service, including federal data/metadata and system data/metadata.* | *Identify the security impact level of the data (Low, Moderate, or High) in accordance with FIPS 199.* | *Build maps which can include routes and traffic information.* |
| *CSO B API* | *TCP/NN* | *API Key, OAuth 2* |  |  |  | *Run web apps on CSO B infrastructure* |
| *CSO C API* | *TCP/NN* |  |  |  |  | *Allows an application to connect CSO C service or embed parts of CSO C user experience* |
| *CSO D CLI* | *TCP/NN* |  |  |  |  | *Main commands for building and designing a data center Layer 2 and Layer 3 infrastructure* |
| *CSO E API* | *TCP/NN* |  |  |  |  | *CIM API provides a Common Information Model (CIM) interface for building management applications* |

Trusted Internet Connection (TIC) [SC-7(3)]

|  |
| --- |
| ***Instructions:*** |
| Describe the CSP’s ability to support an agency customer’s TIC requirements.  Delete instruction text after completion. |

Data Flow Diagrams

|  |
| --- |
| ***Instructions:*** |
| *Insert 3PAO-validated data flow diagram(s) and provide a written description of the data flows. The diagram(s) must address all components reflected in the ABD. At a minimum, SSPs should include diagrams for the following logical data flows:*   * *Customer user and customer admin authentication, including the type of multifactor authentication (MFA),* * *CSP administrative and support personnel authentication, including the type of MFA,* * *System application data flow within the authorization boundary, and* * *System application data flow to/from:*   + *External services, including corporate shared services,*   + *Interconnected systems,*   + *Alternate processing sites and backup storage,*   + *Development/Test environment.*   *Each data flow diagram (DFD) should explicitly identify:*   * *Everywhere (internal & external) federal data and metadata at rest and in transit is not protected through encryption,* * *Everywhere data is protected through encryption, and* * *Whether or not the encryption uses FIPS-validated cryptographic modules.*   + ***NOTE:*** *FIPS validation applies to cryptographic modules, not protocols (e.g., TLS). The cryptographic module that sets up the TLS tunnel must be FIPS validated.*   Delete instruction text after completion. |

***NOTE:*** *The data flow diagram must be easily attributable to the ABD illustrated in Section 3-1. The data flow diagram must be easy to read (high resolution) and understand. The encryption and directional arrows for the data flows and stores must be on the diagram or represented via the legend. If necessary, adjust the page orientation to landscape and/or use multiple diagrams to provide the best representation of the data flows. If the diagram is complex, you may create a high-resolution diagram on a larger page size and embed the item in this section.*

Separation Measures [AC-2, AC-4, SC-7]

|  |
| --- |
| ***Instructions:*** |
| *Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships. There are additional capabilities required for separation measures in Table 4-4, #8, and #9. If the 3PAO chooses to refer back to this section from #8 and #9, this section must answer the capabilities requirements for both #8 and #9.*  *The 3PAO must base the assessment of separation measures on strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The 3PAO must describe methods used to verify the strength of separation measures. The security implemented to meet separation requirements should explicitly mention the subnet requirements from SC-7.*  Delete instruction text after completion. |

1. Capability Readiness

Federal Mandates

This section identifies federal requirements applicable to all FedRAMP Authorized CSOs. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 4.2,FedRAMP Requirements*,* below.

|  |
| --- |
| ***Instructions:*** |
| *Only answer “Yes” if the requirement is fully and strictly met. The 3PAO must answer “No” if an alternative implementation is in place. For the FIPS-validated encryption, FedRAMP expects all moderate and above federal data and metadata to be encrypted internally, externally, and traversing the service boundary. The exceptions to this are “organizationally defined” (i.e., organization is typically the CSP in the SSP template) data at rest and data in transit that may not require encryption.*  Delete instruction text after completion. |

*Table 4-1. Federal Mandates*

| # | Compliance Topic | Fully Compliant? | |
| --- | --- | --- | --- |
| Yes | No |
| 1 | Are FIPS 140-validated cryptographic modules (IAW SC-13) consistently used everywhere cryptography is required? This includes all SC-8, SC-8(1), and SC-28 required encryption. |  |  |
| 2 | Does the system fully support user authentication via agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials? |  |  |
| 3 | Is the system operating at Digital Identity Level 2 or higher? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | Does the CSP have the ability to consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | Does the CSP and system meet federal records management requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? [<https://www.archives.gov/records-mgmt/grs>; PL 104-231, 5 USC 552] |  |  |
| 6 | Does the system’s external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances? This applies to the controls SC-20, SC-21, and SC-22 in the SSP. |  |  |

FedRAMP Requirements

This section identifies additional FedRAMP Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

* + 1. Approved Cryptographic Modules [SC-13]

|  |
| --- |
| ***Instructions:*** |
| *The RAR requires that the 3PAO validates that FIPS-validated encryption is used for all data flows and stores, internally, externally, and traversing the system boundary. Therefore, the 3PAO must ensure active FIPS 140-2 or 140-3* ***Validated*** *cryptographic modules are used. FIPS 140-2 or 140-3* ***Compliant is not*** *sufficient. The 3PAO may add rows to the table if appropriate but must not remove the original rows. The 3PAO must identify all non-validated cryptographic modules in use. In the Rev. 5 edition of the FedRAMP System Security Plan Template, the FedRAMP PMO includes an “Appendix Q Cryptographic Modules Table”. The RAR does not require that this Appendix Q be populated but the CSP should be aware of the usefulness of using this Appendix Q to get a handle on their system cryptography. The 3PAO can use this Appendix Q if it is available but otherwise must use Readiness Assessment expertise to determine if this FIPS-validated encryption requirement is fully met by this system. Please see Table 4-2, below.*  Delete instruction text after completion. |

*Table 4-2. Cryptographic Modules*

| # | Cryptographic Module Type | FIPS 140-validated? | | Describe Any Alternative Implementations (If Applicable) | Describe Missing Elements or N/A Justification |
| --- | --- | --- | --- | --- | --- |
| Yes | No |
| 1 | Data at Rest [SC-28] |  |  |  |  |
| 2 | Transmission [SC-8 (1), SC-12, SC-13] |  |  |  |  |
| 3 | Remote Access [AC-17 (2)] |  |  |  |  |
| 4 | Authentication [IA-5 (1)] |  |  |  |  |

* + 1. Transport Layer Security [NIST SP 800-52, most current revision]

|  |
| --- |
| ***Instructions:*** |
| *The 3PAO must identify all protocols in use for both internal and external communications. The 3PAO may add rows to the table if appropriate but must not remove the original rows.*  *Encryption protection of data-at-rest through encryption includes databases; the responsibility for this depends on the service model and the delineation of responsibility between the CSP and customer.*  Delete instruction text after completion. |

*Table 4-3. Transport Layer Security*

| # | The Cryptographic Module Type | Protocol In Use? | | If “yes,” please describe use for both internal and external communications |
| --- | --- | --- | --- | --- |
| Yes | No |
| 1 | SSL (Non-Compliant) |  |  | 1 |
| 2 | TLS 1.0 (Non-Compliant) |  |  | 2 |
| 3 | TLS 1.1 (Non-Compliant) |  |  | 3 |
| 4 | TLS 1.2 (Compliant) |  |  | 4 |
| 5 | TLS 1.3 (Compliant) |  |  | 5 |

* + 1. Identification, Authentication, and Access Control

|  |
| --- |
| ***Instructions:*** |
| *Only answer “Yes” if the answer is consistently “Yes.” For partially implemented areas, answer “No” and describe what is missing to achieve a “Yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described. Please state the capability and method used to determine whether it is in place.*  *This section assumes that the service/system has automation for identification, authentication, and access control in place and operating as intended. FedRAMP allows a bit of leeway if the documentation is not entirely in place describing these capabilities.*  Delete instruction text after completion. |

*Table 4-4. Identification, Authentication, and Access Control*

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- | --- |
| 1 | Does the system support federal user authentication via CAC/PIV credentials? [IA-8(1)] |  |  |  |
| 2 | Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2, IA-4, IA-4(4)] |  |  |  |
| 3 | Does the system require MFA for administrative accounts and functions? [IA-2, IA-2(1)] |  |  |  |
| 4 | Does the system fully comply with Digital Identity Level 2 (AAL2, IAL2, FAL2) or higher? [NIST SP 800-63] |  |  | *State the Digital Identity Level and provide sufficient details demonstrating that the system complies with this level, consistent with NIST SP 800-63 and FedRAMP guidance.* |
| 5 | Does the system employ automated mechanisms to support account management? [AC-2(1)] |  |  |  |
| 6 | Does the system restrict non-authorized personnel’s access to resources? [AC-6(2)] |  |  |  |
| 7 | Does the system restrict non-privileged users from performing privileged functions? [AC-6(10)] |  |  |  |
| 8 | Does the system ensure secure separation of customer data? [SC-4] |  |  | *The capability description is not required here, but must be included in Section 3.7, Separation Measures.* |
| 9 | Does the system ensure secure separation of customer processing environments? [SC-2] |  |  | *The capability description is not required here, but must be included in Section 3.7, Separation Measures.* |
| 10 | Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2(7)] |  |  |  |

* + 1. Audit, Alerting, Malware, and Incident Response

|  |
| --- |
| ***Instructions:*** |
| *Only answer “Yes” if the answer is consistently “Yes.” For partially implemented areas, answer “No” and describe what is missing to achieve a “Yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described. Please state the capability and method used to determine whether it is in place.*  *This section assumes that the service/system has automation and a SIEM in place for auditing, alerting, malware, and incident response in place and all are operating as intended. FedRAMP allows a bit of leeway if the documentation is not entirely in place describing these capabilities.*  Delete instruction text after completion. |

*Table 4-5. Audit, Alerting, Malware, and Incident Response*

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- | --- |
| 1 | Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3, MA-3 (2)] |  |  |  |
| 2 | Does the system protect audit information from unauthorized access, modification, and deletion? [AU-7, AU-9] |  |  |  |
| 3 | Does the CSP have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-7, SI-7 (7)] |  |  |  |
| 4 | Does the CSP have an Incident Response Plan and a fully developed Incident Response Test Plan? [IR-3, IR-8] |  |  |  |
| 5 | Does the CSP have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11, SA-11 (1)] |  |  | *If the system contains no custom software development, do not answer “Yes” or “No.” Instead, state “NO CUSTOM CODE” here.* |
| 6 | Does the CSP implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)] |  |  |  |
| 7 | Does the CSP retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-7, AU-7 (1), AU-11] |  |  |  |
| 8 | Does the CSP have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [*FedRAMP Incident Communications Procedure*] |  |  |  |
| 9 | Has the CSP architected the system to allow the external DNS server to reply with valid DNSSEC responses [SC-20]? |  |  |  |
| 10 | Has the CSP ensured that the recursive server is within a FedRAMP Authorized boundary [SC-21]? |  |  |  |
| 11 | Has the CSP enabled DNSSEC requests, for domains outside the boundary, so that DNS calls maintain DNSSEC authentication and integrity [SC-20, SC-21]? |  |  |  |

* + 1. Contingency Planning and Disaster Recovery

|  |
| --- |
| ***Instructions:*** |
| *Only answer “Yes” if the answer is consistently “Yes.” For partially implemented areas, answer “No” and describe what is missing to achieve a “Yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described. Please state the capability and method used to determine whether it is in place.*  *This section assumes that the service/system has automation for contingency planning and disaster recovery in place and all are operating as intended. FedRAMP allows a bit of leeway if the documentation is not entirely in place describing these capabilities.*  Delete instruction text after completion. |

*Table 4-6. Contingency Planning and Disaster Recovery*

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (3), CP-9, CP-10] |  |  |  |
| 2 | Does the CSP have a Contingency Plan and a fully developed Contingency Plan Test Plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8] |  |  |  |
| 3 | Does the system have alternate storage and processing facilities? [CP-6, CP-7] |  |  |  |
| 4 | Does the system have primary and alternate telecommunications services from different providers? [CP-8, CP-8 (2)] |  |  |  |
| 5 | Does the system have backup power generation or other redundancy? [PE-11] |  |  |  |
| 6 | Does the CSP have SLAs in place with all telecommunications providers? [CP-8 (1)] |  |  |  |

* + 1. Configuration and Risk Management

|  |
| --- |
| ***Instructions:*** |
| *Only answer “Yes” if the answer is consistently “Yes.” For partially implemented areas, answer “No” and describe what is missing to achieve a “Yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described. Please state the capability and method used to determine whether it is in place.*  *This section assumes that the service/system has automation for configuration and risk management in place and all are operating as intended. FedRAMP allows a bit of leeway if the documentation is not entirely in place describing these capabilities.*  Delete instruction text after completion. |

*Table 4-7. Configuration and Risk Management*

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP maintain a current, complete, and accurate baseline configuration of the information system? [CM-2] |  |  |  |
| 2 | Does the CSP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8] |  |  |  |
| 3 | Does the CSP have a configuration management plan? [CM-9, CM-11] |  |  |  |
| 4 | Does the CSP follow a formal change control process that includes a security impact assessment? [CM-3, CM-4] |  |  |  |
| 5 | Does the CSP employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)] |  |  |  |
| 6 | Does the CSP prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)] |  |  |  |
| 7 | Does the CSP establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6] |  |  | *If “yes,” describe whether the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or “most restrictive consistent with operational requirements.”* |
| 8 | Does the CSP ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6] |  |  |  |

|  |
| --- |
| ***Instructions:*** |
| For the following questions, 3PAOs may use Table 4-12 (Continuous Monitoring Capabilities – Additional Details) to enter the capability descriptions, supporting evidence and missing elements. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 9 | Does the CSP perform authenticated operating system/ infrastructure, web, database, and container vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5), SI-2(2)] |  |  | *Describe how the 3PAO validated that vulnerability scans were fully authenticated.* |
| 10 | Does the CSP demonstrate the capability to remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days? [RA-5, FedRAMP Continuous Monitoring Guide] |  |  | *Describe how the 3PAO validated that the CSP remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days.* |

* + 1. Data Center Security

|  |
| --- |
| ***Instructions:*** |
| *Only answer “Yes” if the answer is consistently “Yes.” For partially implemented areas, answer “No” and describe what is missing to achieve a “Yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described. Please state the capability and method used to determine whether it is in place.*  Delete instruction text after completion. |

*Table 4-8. Data Center Security*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| 1 | Does the CSP restrict physical system access to only authorized personnel? [PE-2 through PE-6 (except PE-3(1)), PE-8] |  |  |  |
| 2 | Does the CSP monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8] |  |  |  |
| 3 | Does the CSP monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)] |  |  |  |

* + 1. Policies, Procedures, and Training

|  |
| --- |
| ***Instructions:*** |
| *Identify missing policies and procedures. For any family with a policy or procedure gap, please describe the gap below.*  Delete instruction text after completion. |

*Table 4-9. Missing Policy and Procedure Elements*

| **Missing Policy and Procedure Elements** |
| --- |
|  |

|  |
| --- |
| ***Instructions:*** |
| The 3PAO must answer the question below.  Delete instruction text after completion. |

*Table 4-10. Security Awareness Training*

| Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- |
| Does the CSP train personnel on security awareness and role-based security responsibilities? |  |  |  |

Additional Capability Information

FedRAMP will evaluate the responses in this section on a case-by-case basis relative to a FedRAMP Ready designation decision.

* + 1. Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a FedRAMP Readiness decision, especially for larger systems. Please note that once a CSO has been designated FedRAMP Ready, architectural, boundary or other significant changes may invalidate the CSO's FedRAMP Ready designation (a FedRAMP Ready designation and corresponding RAR are valid for one year).

|  |
| --- |
| ***Instructions:*** |
| The 3PAO must answer the questions below.  Delete instruction text after completion. |

*Table 4-11. Change Management*

| # | Question | Yes | No | If “No,” please describe how this function is accomplished. |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP’s change management capability include a fully functioning Change Control Board (CCB)? |  |  |  |
| 2 | Does the CSP have and use development and/or test environments to verify changes before implementing them in the production environment? |  |  |  |

* + 1. Continuous Monitoring (ConMon) Capabilities

|  |
| --- |
| ***Instructions:*** |
| *In the tables below, please describe the current state of the CSP’s ConMon capabilities, as well as the length of time the CSP has been performing ConMon for this system.*  Delete instruction text after completion. |

*Table 4-12. Continuous Monitoring Capabilities*

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
| --- | --- | --- | --- | --- |
| 1 | Does the CSP have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period? |  |  |  |
| 2 | Does the CSP have the ability to scan all hosts in the inventory? |  |  |  |
| 3 | Does the CSP have the ability to provide scan files in a structured data format, such as CSV, XML, or .nessus files? |  |  |  |
| 4 | Is the CSP properly maintaining their Plan of Action and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items? |  |  |  |

|  |
| --- |
| ***Instructions:*** |
| *In the table below, provide any additional details the 3PAO believes to be relevant to FedRAMP’s understanding of the CSP’s continuous monitoring capabilities. If the 3PAO has no additional details, please state “None.”*  Delete instruction text after completion. |

*Table 4-13. Continuous Monitoring Capabilities – Additional Details*

| Continuous Monitoring Capabilities – Additional Details |
| --- |
|  |

* + 1. Status of System Security Plan (SSP)

|  |
| --- |
| ***Instructions:*** |
| *In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the CSP has not yet developed. If the maturity of the SSP is low, or there is a high percentage that is not complete, please describe any risks the 3PAO believes this introduces to a full assessment.*  Delete instruction text after completion. |

*Table 4-14. Maturity of the System Security Plan*

| Maturity of the System Security Plan |
| --- |
|  |

|  |
| --- |
| ***Instructions:*** |
| *In the table below, state the number of controls identified as “Not Applicable” in the SSP. List the control identifier for each, and indicate whether a justification for each has been provided in the SSP control statement. The 3PAO should indicate whether they agree that the control is “Not Applicable” and why.*  Delete instruction text after completion. |

*Table 4-15. Controls Designated “Not Applicable”*

|  |
| --- |
| <x> Controls are Designated “Not Applicable” |
|  |

|  |
| --- |
| ***Instructions:*** |
| *In the table below, state the number of controls with an alternative implementation. List the control identifier for each. The 3PAO should indicate whether they agree that the alternative implementation meets the control requirement and why.*  Delete instruction text after completion. |

*Table 4-16. Controls with an Alternative Implementation*

|  |
| --- |
| <x> Controls have an Alternative Implementation |
|  |