|  |
| --- |
| FedRAMP New CLoud Service or Feature On-Boarding Form Cloud Service Provider NameInformation System NameService or Feature NameVersion #Version Date |



# Executive Summary

The purpose of this document is to provide the necessary information for the Authorizing Official (AO) to make a risk-based decision regarding <**Cloud Service Provider**>’s eligibility to use the FedRAMP New Cloud Service or Feature On-boarding process for specified services and features. The procedures and requirements described in this document are in accordance with the FedRAMP Significant Change Policies and Procedures, available on the FedRAMP website at [www.fedramp.gov](http://www.fedramp.gov). **Please read the FedRAMP Significant Change Policies and Procedures carefully before using this template to determine applicability and appropriateness.**

The Federal Risk and Authorization Management Program (FedRAMP) considers new services or features to be significant changes that may qualify for the specialized FedRAMP New Cloud Service or Feature On-boarding process. FedRAMP requires Cloud Service Providers, desiring to use this process, to undergo an evaluation period before being approved to use this process for future on-boarding requests of specified cloud services and features.

*Instruction:* With regard to “<types of services and features>” below, what constitutes a type of service or features is defined by the CSP. The CSP will provide this definition in Section 2.1 of this document.

The evaluation to approve the Cloud Service Provider (CSP) to use the New Cloud Service or Feature On-boarding process involves two subsequent service or feature requests. Approval to use the New Cloud Service or Feature on-boarding process for <types of services and features> <was achieved on m/d/yyyy is currently pending>. The current status of the evaluation period is included in Table ES‑1 below. This is a living document until the evaluations of the two services or features are complete.

Table ES-1 below identifies the timing and outcome of assessments required to determine if the CSP qualifies for the FedRAMP New Cloud Service or Feature on-boarding process. When all outcomes are satisfied and approved by the AO, the CSP in turn has been approved to use the New Cloud Service or Feature on-boarding process for future on-boarding requests of certain services and features. This means that the AO has confidence that:

1. Future services or features will have no impact on existing and already authorized architecture and controls (these will remain static).
2. Future services or features will not require service-specific or feature-specific controls to be added. All NIST SP 800-53 security controls required for the new service or feature are in the existing and already authorized architecture and security controls.
3. The CSP Configuration Management (CM) and System Development Lifecycle (SDLC) capabilities are mature and ensure no impact on existing architecture and controls (these will remain static) as new services or features are on-boarded.
4. Continuous Monitoring (ConMon) activities will remain un-affected and compliant as new services or features are on-boarded.

Table ES‑1 Qualifying Assessments

| IA Validation | Date | Outcome | AO Approval |
| --- | --- | --- | --- |
| Static Architecture & Controls (1 of 2)  | <**m/d/yyyy**> | <**Satisfied/Other-Than-Satisfied/Pending>** | <**m/d/yyyy/Pending**> |
| Static Architecture & Controls (2 of 2) | <**m/d/yyyy/Pending**> | <**Satisfied/Other-Than-Satisfied/Pending>** | <**m/d/yyyy/Pending**> |
| CSP CM and SDLC (1 of 2) | <**m/d/yyyy**> | <**Satisfied/Other-Than-Satisfied/Pending>** | <**m/d/yyyy/Pending**> |
| CSP CM and SDLC (2 of 2) | <**m/d/yyyy/Pending**> | <**Satisfied/Other-Than-Satisfied/Pending>** | <**m/d/yyyy/Pending**> |
| CSP ConMon (1 of 2) | <**m/d/yyyy/Pending**> | <**Satisfied/Other-Than-Satisfied/Pending>** | <**m/d/yyyy/Pending**> |
| CSP ConMon (2 of 2) | <**m/d/yyyy**> | <**Satisfied/Other-Than-Satisfied/Pending>** | <**m/d/yyyy/Pending**> |

Template Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Template Version | Author |
| 11/8/2016 | Initial document | 1.0 | FedRAMP PMO |
| 3/9/2017 | PMO Quality Review | 2.0 | FedRAMP PMO |
| 6/6/2017 | Updated logo | 2.0 | FedRAMP PMO |
| 8/28/2018 | Annual Review and Update to clarify processes | 3.0 | FedRAMP PMO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Revision History**

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

# About this document

This document template is developed for Independent Assessors (IAs) to report their assessment of a Cloud Service Provider’s (CSP’s) eligibility to use the FedRAMP New Cloud Service or Feature On-boarding process. IAs must edit this template to create the report.

This document uses the term authorizing official (AO) and IA. For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says Agency AO and IA refers primarily to a FedRAMP accredited Third Party Assessment Organization (3PAO). For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging Agency’s AO.

# Who should use this document?

This document is intended to be used by IAs to report their assessment of a CSP’s eligibility to use the FedRAMP New Cloud Service or Feature On-boarding process. U.S. government authorization officials may use the completed version of this document to make risk-based decisions.

# How to contact us

Questions about FedRAMP or this document may be directed to *info@fedramp.gov**.*

For more information about FedRAMP, visit the website at <https://www.fedramp.gov>

TABLE OF CONTENTS

[Executive Summary i](#_Toc522515710)

[About this document iv](#_Toc522515711)

[Who should use this document? iv](#_Toc522515712)

[How to contact us iv](#_Toc522515713)

[1. Introduction 3](#_Toc522515714)

[1.1. Applicable Laws and Regulations 3](#_Toc522515715)

[1.2. Applicable Standards and Guidance 3](#_Toc522515716)

[1.3. Purpose 4](#_Toc522515717)

[1.4. Scope 4](#_Toc522515718)

[2. System Overview 6](#_Toc522515719)

[2.1. Security Categorization 6](#_Toc522515720)

[2.2. System Description 6](#_Toc522515721)

[2.3. Purpose of System 6](#_Toc522515722)

[2.4. New Service(s) or Feature(s) 7](#_Toc522515723)

[2.5. Static Architecture and Controls Description 7](#_Toc522515724)

[2.6. Configuration Management & System Development Lifecycle (SDLC) 8](#_Toc522515725)

[2.7. CSP Continuous Monitoring 8](#_Toc522515726)

[3. On-Boarding Assessment 9](#_Toc522515727)

[3.1. Validation of static architecture and controls 9](#_Toc522515728)

[3.1.1. Methodology and Findings 9](#_Toc522515729)

[3.2. Validation of CM and SDLC 10](#_Toc522515730)

[3.2.1. Methodology and Findings 10](#_Toc522515731)

[3.3. Validation of Continuous Monitoring 11](#_Toc522515732)

[3.3.1. Methodology 11](#_Toc522515733)

[4. Service/Feature Security Assessment 13](#_Toc522515734)

[5. Attestation and Recommendation 13](#_Toc522515735)

[Appendix A – Acronyms 14](#_Toc522515736)

[Appendix B – Infrastructure Scan Results 15](#_Toc522515737)

[Infrastructure Scans: Inventory of Items Scanned 15](#_Toc522515738)

[Infrastructure Scans: Raw Scan Results 15](#_Toc522515739)

[Infrastructure Scans: False Positive Reports 16](#_Toc522515740)

[Appendix C – Database Scan Results 17](#_Toc522515741)

[Database Scans: Raw Scan Results 17](#_Toc522515742)

[Database Scans: Inventory of Databases Scanned 17](#_Toc522515743)

[Database Scans: False Positive Reports 17](#_Toc522515744)

[Appendix D– Web Application Scan Results 19](#_Toc522515745)

[Web Applications Scans: Raw Scan Results 19](#_Toc522515746)

[Web Applications Scans: False Positive Reports 19](#_Toc522515747)

[Appendix E – Other Scan Results 20](#_Toc522515748)

[Other Automated & Misc. Tool Results: Tools Used 20](#_Toc522515749)

[Other Automated & Misc. Tool Results: Inventory of Items Scanned 20](#_Toc522515750)

[Other Automated & Misc. Tool Results: Raw Scan Results 20](#_Toc522515751)

[Other Automated & Other Misc. Tool Results: False Positive Reports 21](#_Toc522515752)

[Unauthenticated Scans 21](#_Toc522515753)

[Unauthenticated Scans: False Positive Reports 22](#_Toc522515754)

[Appendix F – Auxilary Documents 23](#_Toc522515755)

List of Tables

[Table ES‑1 Qualifying Assessments ii](#_Toc522284342)

[Table 1‑1. Information System Unique Identifier, Name and Abbreviation 2](#_Toc522284343)

[Table 1‑2. Service/Feature Name and Abbreviation 3](#_Toc522284344)

[Table 1‑3. Site Names and Addresses 3](#_Toc522284345)

[Table 3‑1. Initial Validations 7](#_Toc522284346)

[Table 3‑2. Static Control Analysis 7](#_Toc522284347)

[Table 3‑3. Configuration Management Control Mechanisms 8](#_Toc522284348)

[Table 3‑4. Change Management Questions 9](#_Toc522284349)

[Table 3‑5. Performance Management Questions 9](#_Toc522284350)

[Table 4‑1. Service/Feature Security Assessments 11](#_Toc522284351)

[Table 4‑2. Service/Feature Security Assessments Questions 11](#_Toc522284352)

[Table B‑1. Infrastructure Scans: False Positive Reports 14](#_Toc522284353)

[Table C‑1. Inventory of Databases Scanned 15](#_Toc522284354)

[Table C‑2. Database Scans: False Positive Reports 16](#_Toc522284355)

[Table D‑1. Inventory of Web Applications Scanned 17](#_Toc522284356)

[Table D‑2. Web Application Scans: False Positive Reports 17](#_Toc522284357)

[Table E‑1. Other Automated & Misc. Tool Results 18](#_Toc522284358)

[Table E‑2. Other Automated & Misc. Tool Results: False Positive Reports 19](#_Toc522284359)

[Table E‑3. Unauthenticated Scans 19](#_Toc522284360)

[Table E‑4. Infrastructure Scans: False Positive Reports 20](#_Toc522284361)

# Introduction

This document consists of the results of the comprehensive assessment of **<CSP Name>**’s eligibility to use the FedRAMP New Cloud Service or Feature On-boarding process. This assessment report, and the results documented herein, is provided in support of <**CSP name**> Security Authorization program goals, efforts, and activities necessary to ensure compliance with FedRAMP security requirements. This report describes the outcome of assessments to determine if current and future on-boarding of certain <**CSP name**> services or features qualify for the FedRAMP Service Offering or Feature On-boarding process.

## Applicable Laws and Regulations

* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* E-Authentication Guidance for Federal Agencies [OMB M-04-04]
* Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
* Freedom of Information Act as Amended in 2002 [PL 104-232, 5 USC 552]
* Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization and Protection [HSPD-7]
* Internal Control Systems [OMB Circular A-123]
* Management of Federal Information Resources [OMB Circular A-130]
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Privacy Act of 1974 as amended [5 USC 552a]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Records Management by Federal Agencies [44 USC 31]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

## Applicable Standards and Guidance

* A NIST Definition of Cloud Computing [NIST SP 800-145]
* Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
* Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A, Revision 1]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
* Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]
* Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
* Managing Information Security Risk: Organization, Mission, and Information System View [NIST SP 800-39]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-2]
* Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
* Guide for Conducting Risk Assessments [NIST SP 800-30, Revision 1]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
* Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

## Purpose

This request and its underlying assessment are intended to enable FedRAMP to reach an approval decision to permit CSPs to use the FedRAMP New Cloud Service or Feature On-boarding process to on-board certain types of services or features. The approval decision is based on the maturity of the organizational processes and nature (static and inheritable) of the existing and authorized cloud service architecture and security controls.

FedRAMP requires CSPs to use IAs to perform independent assessment testing and development of this report. This assessment was performed by <**IA**>.

## Scope

The <**system name**> received a <**JAB-PATO/ATO** > on <**date**>. The <**system** **name**>has a unique identifier which is noted in Table 1-1. This report includes information on the service(s) or feature(s) specified in Table 1-2.

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

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
|  |  |  |

*Instruction: Please add rows as necessary.*

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

Table 1‑2. Service/Feature Name and Abbreviation

| Service or Feature Name | Service of Feature Abbreviation |
| --- | --- |
|  |  |

Documentation used by the IA to perform this evaluation includes the following:

*Instruction: Please add-to or revise the list with all that apply.*

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

* <**system name**> *System Security Plan*
* <**system name**> *Contingency Plan & Test Results*
* <**system name**> *Incident Response Plan & Test Results*
* <**system name**> *Configuration Management Plan*
* <**system name**> *Vulnerability Scan Reports*
* <**system name**> *Awareness and Training Reports*
* <**system name**> *Authorization Package*

The <**system name**> and services/features noted in Table 1-2 is physically located at the facilities noted in Table 1-3.

Table 1‑3. Site Names and Addresses

| Data Center Site Name | Address | Description of Components |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# System Overview

## Security Categorization

The **<Information System Name>** is categorized as a **<Low/Moderate/High>** impact system. The **<Information System Name>** categorization is determined in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

## System Description

*Instruction: In the section below, insert a general description of the information system. Use a description that is consistent with the description found in the System Security Plan (SSP). The description should only differ from the description in the SSP if additional information is going to be included that is not available in the SSP or if the description in the SSP is not accurate.*

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

## Purpose of System

*Instruction: In the section below, insert the purpose of the information system. Ensure that the purpose is consistent with the one in the System Security Plan.*

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

## New Service(s) or Feature(s)

*Instruction: In the section below:*

* *Insert a description of the new service or feature that is part of the evaluation.*
* *Describe the type of service or feature.*
* *Provide the definition of the terms “service” or “feature” from the CSP’s perspective.*
* *What constitutes a type of service or feature is defined by the CSP. Please describe in this section what constitutes a type of service or feature.*
* *Describe the purpose of the new service or feature.*
* *Include illustrative diagrams (network and dataflow). All diagrams must have supporting descriptions (textual walk-though of the diagrams).*
* *The diagrams must:*
	+ *Clearly defined system authorization boundary;*
	+ *Clearly define where the new service resides within the boundary;*
	+ *Depict the location of all major components (software/virtual components) of the new service or feature within the boundary; and*
	+ *Identifies all interconnected internal and external services inside the boundary*
* *The dataflow must:*
	+ *Identify where Federal data is to be processed, stored, or transmitted through the new service or feature;*
	+ *Identify how data comes into and out of the new service; and*
	+ *Identify how all ports, protocols, and services of all inbound and outbound traffic for the service or feature are represented and managed.*

***Please note:*** *If the new service or feature uses different ports, protocols, and/or services than identified within the front matter of the existing SSP, the new feature or service may not use the New Services or Features on-boarding process.*

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

## Static Architecture and Controls Description

*Instruction: In the section below describe in detail the elements and nature of the system that ensures the current architecture, controls, and processes will remain unchanged (static) as certain types of services/features are on-boarded. The definition of a static architecture and control is in the first paragraph of this section. Please include illustrative diagrams. All diagrams must have supporting descriptions (textual walk-throughs of the diagrams).*

*Key considerations: The 3PAO will evaluate this information to ensure there is no impact to static architecture and controls. The 3PAO’s evaluation is included in designated areas of this report.*

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

FedRAMP identifies certain controls and system elements, in the context of new services or features, as static. Static architecture and controls are the set of existing system elements and security controls (procedural, management, operational, and technical) for which the implementation results in a security capability that is inheritable by multiple planned services or features. These controls were independently assessed as part of the cloud service authorization and remain strictly unaffected/ unchanged by the implementation of certain types of services/features. The new service or feature will not require service-specific or feature-specific controls to be added. All controls needed to protect the new service or feature are in the existing and authorized architecture and controls and are inherited as-is (unchanged) by the service/feature.

## Configuration Management & System Development Lifecycle (SDLC)

*Instruction: In the section below, include an illustrative diagram(s) and a supporting description of the CSP configuration management (CM) process and SDLC in relation to new service/feature on-boarding. The description and diagrams must easily correlate.*

*Key considerations: It is critical that CM and SDLC processes are robust. A strong CSP change management capability indicates a more mature change management capability, and influences a FedRAMP approval decision, especially for larger systems where the service is integrated into the SDLC. The 3PAO will validate the automated configuration management mechanisms employed to determine 1) the robustness and maturity of these capabilities, 2) if they can be relied upon by the 3PAO to determine if impacts of changes to the environment are able to be fully known and understood, and 3) if they can be used by the 3PAO to confirm that the existing architecture and controls remain unchanged with current and future on-boarding of new services and features. The 3PAO’s evaluation will not be in this section but another designated area of this report.*

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

## CSP Continuous Monitoring

*Instruction: In the section below, provide an overview of CSP continuous monitoring processes.*

*Key considerations: It is critical that new services/feature on-boarding does not impact ongoing continuous monitoring in a negative way. Note that the 3PAO will evaluate the robustness of ConMon process and the ability of the CSP to maintain effective continuous monitoring as it on-boards services/features.*

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

# On-Boarding Assessment

FedRAMP requires specific assessments as part of the FedRAMP New Cloud Service or Feature on-boarding process. These assessments ensure the CSP qualifies to use the new services on-boarding process for future on-boarding requests of specified services and features. <**IA**> validated the CSP capabilities as described below, in order to evaluate the robustness and maturity of these capabilities. The validations occur as part of two subsequent on-boarding efforts.

Table 3‑1. Initial Validations

|  |  |  |
| --- | --- | --- |
| Validation | Date | Service or Feature Request Name |
| First IA Validation | < m/d/yyyy> | <**First Service or Feature Name**>  |
| Second IA Validation | < m/d/yyyy/Pending> | <**Second Service or Feature Name/Pending**> |

## Validation of static architecture and controls

### Methodology and Findings

<**IA**> validated that 1) the existing architecture and controls (procedural, management, operational, and technical) remain static (strictly unaffected/unchanged) and 2) all controls needed to protect the new service or feature are in the existing and authorized architecture and controls and are inherited by the service/feature as-is (unchanged). This validation occurred for the services or features in Table 3-1, as described below.

*Instruction: The 3PAO must review the system controls to ensure that they remain un-impacted by new service and feature on-boarding. This section contains a static control analysis worksheet that is used to confirm that controls (and architecture) are not added or impacted for two subsequent service/feature requests. The 3PAO must use examine (review evidence) and test methods to establish that controls are not impacted. Evaluation through interviews will not be accepted.*

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

Table 3‑2. Static Control Analysis



## Validation of CM and SDLC

### Methodology and Findings

<**IA**> validated that the CSP CM and SDLC were used as described below. This validation occurred as part of the change request process for the services or features listed in Table 3-1.

<**IA**> validated the automated configuration management mechanisms employed to determine 1) the robustness and maturity of these capabilities, 2) if they can be relied upon by the IA to determine if impacts of changes to the environment are able to be fully known and understood, and 3) if they can be used by the IA to confirm that the existing architecture and controls remain unchanged (no addition of controls or modifications to controls) with current and future on-boarding of the specific type of new services and features described in this report.

*Instruction: Please specify configuration items according to NIST SP 800-128 guidance, which states that:*

* *A configuration item is an aggregation of information system components designated for configuration management and treated as a single entity*
* *A configuration item may be a specific information system component (e.g., server, workstation, router, application), a group of information system components (e.g., group of servers with like operating systems, group of network components such as routers and switches, an application or suite of applications), or a non-component object (e.g., firmware)*

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

Table 3‑3. Configuration Management Control Mechanisms

| Component Category | Configuration Control Mechanism | Mechanism Type (Automated/ Manual) | Results and Compensation for Manual Methods (First Validation) | Results and Compensation for Manual Methods (Second Validation) |
| --- | --- | --- | --- | --- |
| <Configuration Item>  |  |  |  |  |
| <Configuration Item>  |  |  |  |  |
| <Configuration Item>  |  |  |  |  |
| <Configuration Item>  |  |  |  |  |
| <Configuration Item>  |  |  |  |  |
| <Configuration Item>  |  |  |  |  |
| <Configuration Item>  |  |  |  |  |

The <**IA**> also evaluated the services or features in in Table 3-3 based on the following questions.

Table 3‑4. Change Management Questions

| Question | Observations and Evidence (First Validation) | Observations and Evidence (Second Validation) |
| --- | --- | --- |
| Can the CSP’s change management capabilities, as described in Table 3-3, be relied upon by the IA to determine if impacts of changes to the environment are able to be fully known and understood? |  |  |
| Does the CSP’s change management process incorporate the system and security information necessary to assess the security impact of the new service within the existing system boundary?  |  |  |
| Has the change request been approved by the required person(s) with security responsibility for the CSP’s Change Control Board (CCB)? If yes, please provide the date of the approval. |  |  |
| Do the results in the CSP’s test plan demonstrate a successful deployment and integration test of the new service in a development or test environment prior to production deployment?  |  |  |
| Do the security development artifacts provided demonstrate that the vendor has assessed the new service using their existing security development standards and processes? |  |  |

## Validation of Continuous Monitoring

### Methodology

<**IA**> validated that ConMon activities will remain compliant. This validation occurred as part of the change request process for the new services or features listed in Table 3-1.

Table 3‑5. Performance Management Questions

| Question | Observations and Evidence (First Validation) | Observations and Evidence (Second Validation) |
| --- | --- | --- |
| Does the SSP, and supporting documents, clearly and accurately reflect the new service or feature? |  |  |
| Has the CSP documented new customer responsibilities associated with this new service or feature in the Control Implementation Summary (CIS)?  |  |  |
| Does the inventory completely and accurately reflect the new service or feature? |  |  |
| Has the new service or feature been successfully scanned by the CSP? |  |  |
| Has the CSP maintained compliance with the FedRAMP Continuous Monitoring Performance requirement with respect to unique vulnerability count? |  |  |
| Has the CSP maintained compliance with the FedRAMP Continuous Monitoring Performance requirement with respect to scanning requirements in the “FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide?” |  |  |
| Has the CSP maintained compliance with the FedRAMP Continuous Monitoring Performance requirement with respect to remediation of high impact vulnerabilities? |  |  |
| Has the CSP maintained compliance with the FedRAMP Continuous Monitoring Performance requirement with respect to remediation of moderate impact vulnerabilities? |  |  |
| Has the CSP maintained compliance with the FedRAMP Continuous Monitoring Performance requirement with respect to remediation of low impact vulnerabilities? |  |  |
| Has the CSP maintained compliance with the FedRAMP Continuous Monitoring Performance requirement with respect to quality of deliverables - timely or accurate submission of any deliverable, including, but not limited to, monthly ConMon documents, and Deviation Requests? |  |  |

# Service/Feature Security Assessment

<**IA**> performed assessments of the services or features as described in Table 4-1:

Table 4‑1. Service/Feature Security Assessments

| First Validation | Second Validation |
| --- | --- |
| 1. <Appendix A – Infrastructure Scan Results>
2. <Appendix B – Database Scan Results>
3. <Appendix C – Web Application Scan Results>
4. <Appendix D – Other Scan Results>
 | 1. <Appendix A – Infrastructure Scan Results>
2. <Appendix B – Database Scan Results>
3. <Appendix C – Web Application Scan Results>
4. <Appendix D – Other Scan Results>
 |

Table 4‑2. Service/Feature Security Assessments Questions

| Question | Observations and Evidence (First Validation) | Observations and Evidence (Second Validation) |
| --- | --- | --- |
| Does the SSP and supporting documents clearly and accurately reflect the new service or feature? |  |  |
| Has the CSP documented new customer responsibilities associated with this new service or feature in the CIS? |  |  |
| Does the inventory completely and accurately reflect the new service or feature? |  |  |
| Has the new service or feature been successfully scanned by the CSP? |  |  |

# Attestation and Recommendation

<**IA**> attests that 1) this report is complete and accurate and 2) the on-boarding of the new services or features described in this document <meet/failed to meet> all FedRAMP requirements. With regard to <**Cloud Service Name**>’s use of the FedRAMP New Cloud Service or Feature on-boarding process: <**IA**> <will provide its recommendation upon completion of the second (of two) new service or feature on-boarding request evaluations required as part of the eligibility assessment / recommends approval / recommends use of the standard FedRAMP significant change request process>. <Additional rationale for IA attestation and recommendation.>

Appendix A – Acronyms

| Acronym | Definition |
| --- | --- |
| 3PAO | Third Party Assessor Organization |
| AO | Authorizing Official |
| ATO | Authorization to Operate |
| CCB | Change Control Board |
| CIS | Control Implementation Summary |
| CM | Configuration Management |
| CSP | Cloud Service Provider |
| DNS | Domain Name System |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS PUB | Federal Information Processing Standard Publication |
| FISMA | Federal Information Security Management Act |
| FP | False Positive |
| ID | Identification |
| IA | Independent Assessor  |
| IT | Information Technology |
| JAB | Joint Authorization Board |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PIV | Personal Identity Verification |
| POA&M | Plan of Action and Milestones |
| RA | Risk Assessment |
| Rev. | Revision |
| SA | Security Assessment |
| SDLC | System Development Life Cycle |
| SP | Special Publication |
| SSP | System Security Plan |

Appendix B – Infrastructure Scan Results

Infrastructure scans consist of scans of operating systems, networks, routers, firewalls, Domain Name System (DNS) servers, domain servers, NIS masters, and other devices that keep the network running. Infrastructure scans can include both physical and virtual host and devices. The <**tool** **name**, **version**> vulnerability scanner was used to scan the <**system** **name**> network/OS components. <**Number**> percent of the inventory was scanned. For the remaining inventory, the IA technical assessor performed a manual review of configuration files to analyze for existing vulnerabilities.

*Instruction: Documents may be attached as an embedded file or if the file is not embedded and is sent to FedRAMP by other means, provide the title, version, and exact file name, including the file extension.*

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

Infrastructure Scans: Inventory of Items Scanned

*Instruction: The FedRAMP inventory template,* [SSP ATTACHMENT 13 - FedRAMP Integrated Inventory Workbook Template](https://www.fedramp.gov/assets/resources/templates/SSP-A13-FedRAMP-Integrated-Inventory-Workbook-Template.xlsx), *may be found at* [*https://www.fedramp.gov/templates/*](https://www.fedramp.gov/templates/)*.*

*Documents may be attached as an embedded file or if the file is not embedded and is sent to FedRAMP by other means, provide the title, version, and exact file name, including the file extension.*

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

Infrastructure Scans: Raw Scan Results

*Instruction: Provide all fully authenticated infrastructure scan results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.*

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

The following raw scan results files are included:

**<List files here include Title, Filename (including extension)>**

*Instruction: Use the summary table to identify false positives that were generated by the scanner. For each false positive reported, add an explanation as to why that finding is a false positive. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “IS” in the identifier number refers to “Infrastructure Scan.”*

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

Infrastructure Scans: False Positive Reports

Table B‑1. Infrastructure Scans: False Positive Reports

| ID# | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-IS |  |  |  |  |
| 2-FP-IS |  |  |  |  |
| 3-FP-IS |  |  |  |  |
| 4-FP-IS |  |  |  |  |

Appendix C – Database Scan Results

The <**tool** **name**, **version**> vulnerability scanner was used to scan the <**system** **name**> databases. <**Number**>% percent of all databases were scanned.

Database Scans: Raw Scan Results

*Instruction: Provide all database scan results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.*

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

The following raw scan results files are included:

**<List files here include Title, Filename (including extension**)**>**

Database Scans: Inventory of Databases Scanned

*Instruction: Scan 100% of all databases that make up the candidate system unless otherwise approved. Indicate what was scanned in the table that follows. For “Function”, indicate the function that the database plays for the system (e.g., database image for end-user development, database for authentication records). Add additional rows as necessary.*

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

Table C‑1. Inventory of Databases Scanned

| IP Address | Hostname | Software & Version | Function | Comment |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Database Scans: False Positive Reports

*Instruction: Use the summary table to identify false positives that were generated by the scanner. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “DS” in the identifier number refers to “Database Scan.”*

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

Table C‑2. Database Scans: False Positive Reports

| ID# | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-DS |  |  |  |  |
| 2-FP-DS |  |  |  |  |
| 3-FP-DS |  |  |  |  |

Appendix D– Web Application Scan Results

The <**tool** **name**, **version**> vulnerability scanner was used to scan the <**system** **name**> web applications. <**Number**>% of all web applications were scanned.

Table D‑1. Inventory of Web Applications Scanned

| Login URL | IP Address of Login Host | Function | Comment |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Web Applications Scans: Raw Scan Results

*Instruction: Provide all web application scan results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.*

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

The following raw scan results files are included:

**<List files here include Title, Filename (including extension)>**

Web Applications Scans: False Positive Reports

*Instruction: Use the summary table to identify false positives generated by the scanner. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “WS” in the identifier number refers to “Web Application Scan.”*

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

Table D‑2. Web Application Scans: False Positive Reports

| ID# | Scanner Severity Level | Page & IP Address | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-WS |  |  |  |  |
| 2-FP-WS |  |  |  |  |
| 3-FP-WS |  |  |  |  |
| 4-FP-WS |  |  |  |  |

Appendix E – Other Scan Results

<**No Additional/Additional**> automated tools were used during this assessment.

Other Automated & Misc. Tool Results: Tools Used

The <**Scanner Name, Vendor, & Version #**> was used to scan the <**Service or Feature Name**> <**service/feature**>.

The <**Scanner Name, Vendor, & Version #**> was used to scan the <**Service or Feature Name**> <**service/feature**>.

Other Automated & Misc. Tool Results: Inventory of Items Scanned

*Instruction: Provide any additional tests performed using automated tools in this Appendix. Bundle all output from automated tools into one zip file. This Appendix may not be needed if no other automated tools were used. If that is the case, write “Not Applicable” in the first column.*

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

Table E‑1. Other Automated & Misc. Tool Results

| IP Address | Function | Finding | False Positive Explanation |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Other Automated & Misc. Tool Results: Raw Scan Results

*Instruction: Provide the results from all other automated tools. Bundle all reports generated by automated tools into one zip file. Do not insert files that require a license to read the file.*

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

The following raw scan results files are included:

**<List files here include Title, Filename (including extension)>**

## Other Automated & Other Misc. Tool Results: False Positive Reports

*Instruction: Use the summary table to identify false positives that were generated by tools. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “OT” in the identifier number refers to “Other Tools.” If other automated or miscellaneous tools were not used, write “Not Applicable” in the first column. Delete this and all other instructions from your final version of this document.*

Table E‑2. Other Automated & Misc. Tool Results: False Positive Reports

| ID# | IP Address | Tool/Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-OT |  |  |  |  |
| 2-FP-OT |  |  |  |  |
| 3-FP-OT |  |  |  |  |
| 4-FP-OT |  |  |  |  |

Unauthenticated Scans

*Instruction: Provide the results from any unauthenticated scans. Bundle all reports generated by automated tools into one zip file. Do not insert files that require a license to read the file. In order to use this table, the IA must obtain approval from the AO when submitting the SAP. If this table is not used, write “Not Applicable” in the first column.*

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

Table E‑3. Unauthenticated Scans

| IP Address | Hostname | Software & Version | Function | Comment |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Unauthenticated Scans: False Positive Reports

*Instruction: Use the summary table to identify false positives that were generated by unauthenticated scans. For each false positive reported, add an explanation as to why that finding is a false positive. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “US” in the identifier number refers to “Unauthenticated Scan.“* *If Table E‑3 was not used, do not use this table and write “Not Applicable” in the first column.*

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

Table E‑4. Infrastructure Scans: False Positive Reports

| ID# | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
| 1-FP-US |  |  |  |  |
| 2-FP-US |  |  |  |  |
| 3-FP-US |  |  |  |  |
| 4-FP-US |  |  |  |  |

Appendix F – Auxilary Documents

Auxiliary documents are listed below. All evidence collected as part of the assessment has been posted in <**OMB MAX/Name of CSP Repository**> within the associated evidence zip files.

* <**file name**> <**short description**>
* <**file name**> <**short description**>
* <**file name**> <**short description**>