Agency Authorization Review Report

#N/A

FedRAMP Review for:	(select CSP)		
Recommendation:	(select action)	**Date:**	MM/DD/YYYY
NIST SP 800-53 Revision (Rev 3 or Rev 4):	(select)	**Deployment Model:**	(select)
Document Versions Reviewed:	SSP (vx.x MM/DD/YY), SAP (vx.x MM/DD/YY), SAR (vx.x MM/DD/YY) and POA&M (vx.x MM/DD/YY)		
Assessor (3PAO or Agency Selected):	(enter assessor info)		
Service Model:	(select)	**System Categorization:**	(select)

Section A: Executive Summary

Section B: Documents Provided Check

#	Description	Provided?
1.0	Initial Authorization Package Checklist	----
2.0	System Security Plan (SSP)*	
2.1	Att. 1: Information Security Policies & Procedures*	----
2.2	Att. 2: User Guide	----
2.3	Att. 3: Electronic Authentication (E-Authentication) Plan*	----
2.4	Att. 4: Privacy Impact Assessment (PIA)	----
2.5	Att. 5: Rules of Behavior (ROB)	----
2.6	Att. 6: Information System Contingency Plan (ISCP)*	----
2.7	Att. 7: Configuration Management Plan (CMP)*	----
2.8	Att. 8: Incident Response Plan (IRP)*	----
2.9	Att. 9: Control Implementation Summary (CIS) Workbook	----
2.10	Att. 10: Federal Information Processing Standard (FIPS) 199 Categorization	----
2.11	Att. 11: Separation of Duties Matrix	----
2.12	Att. 12: Laws and Regulations	----
2.13	Att. 13: Integrated Inventory Workbook	----
3.0	Security Assessment Plan (SAP)*	----
3.1	App. A - Security Test Case Procedures	----
3.2	App. B - Penetration Testing Plan and Methodology	----
3.3	App. C - 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement and Sampling Methodology)	----
4.0	Security Assessment Report (SAR) *	----
4.1	App. A - Risk Exposure Table	----
4.2	App. B - Security Test Case Procedures	----
4.3	App. C - Infrastructure Scan Results	----
4.4	App. D - Database Scan Results	----
4.5	App. E - Web Application Scan Results	----
4.6	App. F - Assessment Results	----
4.7	App. G - Manual Test Results	----
4.8	App. H - Documentation Review Findings	----
4.9	App. I - Auxiliary Documents	----
4.10	App. J - Penetration Test Report	----
5.0	Plan of Action and Milestones (POA&M)*	----
6.0	Continuous Monitoring Plan (ConMon Plan)	----
7.0	ATO Letter	----

Other Comments:

Key: ✔ = Doc provided ✖ = Doc not provided * Key Doc (Agency review only)

Section C: Overall SSP Checks

#	Description	Yes/No	Comments
1	Do all controls have at least one implementation status checkbox selected?	----	
2	Are all critical controls implemented?	----	
3	Are the customer responsibilities clearly identified (by checkbox selected and in the implementation description)?	----	
4	Does the Roles Table (User Roles and Privileges) sufficiently describe the range of user roles, responsibilities, and access privileges?	----	
5	In the control summary tables, does the information in the Responsible Role row correctly describe the required entities responsible for fulfilling the control?	----	
6	Was the appropriate e-Authentication Level selected?	----	
7	Is the authorization boundary explicitly identified in the network diagram?	----	

Agency Authorization Review Report

#N/A

8	Is there a data flow diagram that clearly illustrates the flow and protection of data going in and out of the service boundary and including all traffic flows for both internal and external users?	----
9	Are any third-party or external cloud services lacking FedRAMP Authorization used?	
10a	If this is a SaaS or a PaaS, is it "leveraging" another IaaS with a FedRAMP Authorization?	----
10b	If 10a is Yes, are the "inherited" controls clearly identified in the control descriptions?	----
11	Are all interconnections correctly identified and documented in the SSP?	----
12	Are all required controls present?	----
13	Is the inventory provided in the FedRAMP Integrated Inventory Workbook?	----

Other Comments:

Section D: SSP Critical Control Checks

Control	Control	Yes/No	Comments
AC-2	Account Management	----	
AC-4	Information Flow Enforcement	----	
AC-17	Remote Access	----	
CA-1	Security Assessment and Authorization Policies and Procedures	----	
CM-6	Configuration Settings	----	
CP-7	Alternate Processing Site	----	
CP-9	Information System Backup	----	
IA-2(1)	Identification and Authentication (Organizational Users) - network access to privileged accounts.	----	
IA-2(2)	Identification and Authentication (Organizational Users) - for Network Access to Non-privileged Accounts	----	
IA-2(3)	Identification and Authentication - Local Access to Privileged Accounts	----	
IA-2(11)	Identification and Authentication - Remote Access - Separate Device Authentication	----	
IA-2(12)	Identification and Authentication - Acceptance of PIV Credentials	----	
IR-8	Incident Response Plan	----	
RA-5	Vulnerability Scanning	----	
RA-5(5)	Vulner. Scan. - Privileged Access Authorization	----	
RA-5(8)	Vulner. Scan. - Review Historic Audit Logs	----	
SA-11	Developer Security Testing and Evaluation	----	
SA-11(1)	Developer Security Testing and Evaluation - Static Code Analysis	----	
SC-4	Information in Shared Resources	----	
SC-7	Boundary Protection	----	
SC-13	Cryptographic Protection - FIPS-validated or NSA-approved	----	

Other Comments:

Section E: SAP Checks (for CSP and Agency Reviews)

#	Description	Yes/No	Comments
1	FedRAMP SAP template used, including all sections?	----	
2	Security Assessment Test Cases present?	----	
3a	Rules of Engagement present?	----	
3b	Penetration Test Plan present (may be combined with Rules of Engagement)?	----	
4	Is there an inventory of items to be tested?	----	
5	If a sampling methodology was used for technical testing, was the sampling methodology/plan described?	----	

Other Comments:

Agency Authorization Review Report

#N/A

Section F: SAR Checks (for CSP and Agency Reviews)

#	Description	Yes/No	Comments
1	FedRAMP SAR template used, including all sections?	----	
2	Are risks documented?	----	
3	Was evidence provided, or was there a statement that evidence can be provided upon request?	----	
4	Completed Security Assessment Test Cases present and in accordance with FedRAMP template?	----	
5	Security scan results present?	----	
6	Penetration Test Report present and consistent with the SAR?	----	
7	Are deviations from the SAP documented?	----	
8	Does the 3PAO provide an attestation statement or recommendation for authorization?	----	
9	Are there zero High findings identified in the SAR? If there are any high findings, provide number and comments.	----	
10	Are the numbers of risks/findings consistently stated within the SAR, where appropriate?	----	
11	Are the inventory lists within the SAR and SSP consistent?	----	

Other Comments:

Section G: POA&M Checks (for CSP and Agency Reviews)

#	Description	Yes/No	Comments
1	Is the POA&M in the FedRAMP POA&M template?	----	
2	POA&M consistent with SAR Risk Exposure Summary Table	----	
3	Is there an inventory, either in a POA&M Inventory Tab, or in the SSP?	----	

Other Comments: