Agency Authorization Review Report

Get pkg ID from Trello Card

FedRAMP Review for:	**CSP Name**		
Status:	**(select action)**	**Date:**	MM/DD/YYYY
Service Model:	**(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)**	**System Categorization:**	**Moderate**

Section A: Executive Summary

Section B: Documents Provided Check

Key: Issue = Action Required. OK = No action required. N/A = Not applicable for this package.

#	Description	Provided?	#	Description	Provided?
1.0	Initial Authorization Package Checklist	----	**4.0**	**Security Assessment Plan (SAP)***	----
2.0	**ATO Provided**	----	4.1	App. A - Security Test Case Procedures	----
3.0	**System Security Plan (SSP)***	----	4.2	App. B - Penetration Testing Plan and Methodology	----
3.1	Att. 1: Information Security Policies & Procedures*	----	4.3	App. C - 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement and Sampling Methodology)	----
3.2	Att. 2: User Guide	----	**5.0**	**Security Assessment Report (SAR) ***	----
3.3	Att. 3: Digital Identity Level Selection*	----	5.1	App. A - Risk Exposure Table	----
3.4	Att. 4: Privacy Impact Assessment (PIA)	----	5.2	App. B - Security Test Case Procedures	----
3.5	Att. 5: Rules of Behavior (ROB)	----	5.3	App. C - Infrastructure Scan Results	----
3.6	Att. 6: Information System Contingency Plan (ISCP)*	----	5.4	App. D - Database Scan Results	----
3.7	Att. 7: Configuration Management Plan (CMP)*	----	5.5	App. E - Web Application Scan Results	----
3.8	Att. 8: Incident Response Plan (IRP)*	----	5.6	App. F - Assessment Results	----
3.9	Att. 9: Control Implementation Summary (CIS) Workbook	----	5.7	App. G - Manual Test Results	----
3.1	Att. 10: Federal Information Processing Standard (FIPS) 199 Categorization	----	5.8	App. H - Documentation Review Findings	----
3.11	Att. 11: Separation of Duties Matrix	----	5.9	App. I - Auxiliary Documents	----
3.12	Att. 12: Laws and Regulations	----	5.10	App. J - Penetration Test Report	----
3.13	Att. 13: Integrated Inventory Workbook	----	**6.0**	**Plan of Action and Milestones (POA&M)***	----
			7.0	**Continuous Monitoring Plan (ConMon Plan)**	----

Other Comments:

Section C: Overall SSP Checks

#	Description	OK/Issue	Comments
1a	Is the correct SSP Template used?	----	
1b	Is the correct Deployment Model chosen for the system?	----	
2	Do all controls have at least one implementation status checkbox selected?	----	
3	Are all critical controls implemented?	----	
4a	Are the customer responsibilities clearly identified in the CIS - CRM Tab, as well as the SSP Controls (by checkbox selected and in the implementation description)? Are the CIS-CRM and SSP controls consistent for customer responsibilties? A sampling of 7 controls involving customer roles is reviewed.	----	
4b	Does the Initial Authorizing Agency concur with the CRM (adequacy and clarity of customer responsibilities)?	TBD	*Agency to advise during review meeting.*

Agency Authorization Review Report

Get pkg ID from Trello Card

5	Does the Roles Table (User Roles and Privileges) sufficiently describe the range of user roles, responsibilities, and access privileges?	----
6	In the control summary tables, does the information in the Responsible Role row correctly describe the required entities responsible for fulfilling the control?	----
7	Is the appropriate Digital Identity Level selected?	----
8	Is the authorization boundary explicitly identified in the network diagram?	----
9	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?	----
10	Are any third-party or external cloud services lacking FedRAMP Authorization used?	
11a	If this is a SaaS or a PaaS, is it "leveraging" another IaaS with a FedRAMP Authorization?	----
11b	If 11a is Yes, are the "inherited" controls clearly identified in the control descriptions?	----
12	Are all interconnections correctly identified and documented in the SSP?	----
13	Are all required controls present?	----
14	Is the inventory provided in the FedRAMP Integrated Inventory Workbook?	----
15	Is the CSO compliant with DNSSEC? (Controls SC-20 and SC-21 apply)	----
16	Does the CSO adequately employ DMARC (Domain-based Message Authentication, Reporting & Conformance (DMARC) requirements) according to DHS BOD 18-01?	----

Other Comments:

Section D: Moderate SSP Critical Control Checks

Control	Control	OK/Issue	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:

Agency Authorization Review Report

Get pkg ID from Trello Card

Section E: SAP Checks

#	Description	OK/Issue	Comments
1	FedRAMP SAP template used, including all sections?	----	
2	Security Assessment Test Cases (Test Case Workbook) 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:

Section F: SAR Checks

#	Description	OK/Issue	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?	----	
4a	Completed Security Assessment Test Cases present and in accordance with FedRAMP template?	----	
4b	If SSP controls reflect any alternative implementations, do the test cases reflect specific test procedures to address each particular alternative implementation?	----	
5	Security scan results present?	----	
6	Penetration Test Report present and consistent with the FedRAMP Pen Test Guidance?	----	
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?	----	
12	Are SAR test results consistent with FedRAMP Timeliness and Accuracy of Testing Requirements?	----	

Other Comments:

Findings:
High:
Mod:
Low:
 # risks downgraded (by level) due to mitigating factors

Section G: POA&M Checks

#	Description	OK/Issue	Comments
1	Is the POA&M in the FedRAMP POA&M template?	----	
2	POA&M consistent with SAR Risk Exposure Summary Table?	----	
3	Are the POA&M line items consistent with the FedRAMP POA&M Template Completion Guide?	----	
4a	Have any Operationally Required items (ORs) in the POA&M been validated by 3PAO? (Included in the SAR)	----	
4b	Have all ORs risk accepted by the Authorizing Agency?	----	
5	Does the POA&M reflect adherence to FedRAMP time-frame requirements (completion dates by 30 days for High, 90 for Moderate, and 180 days for low vulnerabilities)?	----	

Other Comments:

Controlled Unclassified Information

Agency Authorization Review Report	Get pkg ID from Trello Card

v4.3