Controlled Unclassified Information

DRAFT - Agency Authorization Review Report - DRAFT

FR Package ID#

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

Section A: Executive Summary

Key: Concern = Action may be required. OK = No action required. N/A = Not applicable for this package.

Section B: Documents Provided Check

#	Description	OK/Concern		#	Description	OK/Concern
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)**	----
3.1	Att. 1: Information Security Policies and Procedures	----
3.2	Att. 2: User Guide	----
3.3	Att. 3: Digital Identity Worksheet	----
3.4	Att. 4: Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)	----
3.5	Att. 5: Rules of Behavior (ROB)	----
3.6	Att. 6: Information System Contingency Plan (ISCP)	----
3.7	Att. 7: Configuration Management Plan (CMP)	----
3.8	Att. 8: Incident Response Plan (IRP)	----
3.9	Att. 9: Control Implementation Summary (CIS) Workbook	----
3.10	Att. 10: Federal Information Processing Standard (FIPS) 199 Categorization	----
3.11	Att. 11: Separation of Duties Matrix	----
3.12	Att. 12: FedRAMP Laws and Regulations	----
3.13	Att. 13: FedRAMP Integrated Inventory Workbook	----

4.2	App. B - Penetration Testing Plan and Methodology	----
4.3	App. C - 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement and Sampling Methodology)	----
5.0	**Security Assessment Report (SAR)**	----
5.1	App. A - Risk Exposure Table	----
5.2	App. B - Security Test Case Procedures	----
5.3	App. C - Infrastructure Scan Results	----
5.4	App. D - Database Scan Results	----
5.5	App. E - Web Application Scan Results	----
5.6	App. F - Assessment Results	----
5.7	App. G - Manual Test Results	----
5.8	App. H - Documentation Review Findings	----
5.9	App. I - Auxiliary Documents	----
5.10	App. J - Penetration Test Report	----
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/Concern	Comments
1	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 Worksheet tabs, as well as the SSP controls (by checkbox selected and in the implementation description)? Are the CIS/CRM and SSP controls consistent for customer responsibilities? A sampling of seven 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*
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?	----	
8a	Is the authorization boundary explicitly identified in the network diagram?	----	*An acceptable boundary diagram is a clearly marked boundary (e.g., a labeled box or line around the components included). The diagram must be legible and readable.* *The diagram should:* *• Include a clearly defined authorization boundary,* *• Include system interconnections used to operate and support the intended mission/business functions,* *• Depict every tool, service, or component that is mentioned in the SSP narrative, and controls,* *• Identify those depicted tools, services, or components as either external or internal to the boundary,* *• Identify all interconnected systems, and whether they are FedRAMP Authorized (or not),* *• Depict how CSP and customer/agency access the service (e.g., authentication used to access service),* *• Depict all major software/virtual components (or groups of) within the boundary,* *• Be validated against the inventory,* *• Show alternate processing site, and* *• Show pulling of updates from external services, such as OS, and antivirus updates.* *Supporting text should describe all internal components.*
8b	Does the CSO provide components to run on the client side?	----	

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 that includes all traffic flows for both internal and external users?	----	Data flow diagrams should be consistent with authorization boundary and: • Clearly identify anywhere federal data is to be processed, stored, or transmitted, • Clearly delineate how data comes into and out of the system boundary, • Clearly identify data flows for privileged, non-privileged and customers' access with MFA details, and • Depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed. • For each data flow, clearly depict protective mechanisms (encryption type and FIPS 140-2 validation or use of other alternative implementations such as physical protection via protective distribution systems [PDS]), where applicable. Note: If any data flows are not protected by encryption, the CSP should be prepared to provide the FedRAMP PMO clarifying details so that a risk decision can be made related to FedRAMP authorization: • Identify the data flow(s) and stores that is/are not encrypted, • Describe the impacted data (government data, government metadata, CSP data, etc.), • Sensitivity of the impacted data (Low vs Moderate), • Mitigations in place, • Remediation plan, where appropriate, • Projected date of remediation, where appropriate.
10	Does the CSP use any third-party or external cloud services that lack FedRAMP authorization? If so, please list them.	----	Check throughout the SSP for services specified and if they are in the boundary diagram. ID any services not called out as part of the boundary discussion/diagram.
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?	----	Consistently address the external services referenced in C.10 and C.11a as follows: 1) Table 8-3. Leveraged Authorizations - should contain all FedRAMP Authorized CSOs 2) Tables 11-1. System Interconnections and 13-3. CA-3 Authorized Connections, and SAR Section 6. Risks Known For Interconnected Systems - should catalog all external services 3) SA-9 External Information System Services - should address all external services where federal information is processed or stored 4) Supporting narrative a) Provide a brief description of how each is used in support of the CSO b) Describe the data shared with each external service - particularly those lacking FedRAMP authorization 5)) ABD a) Show how each external service interacts with users and the CSO boundary b) Depict the FedRAMP authorization status for each external service 6) DFD - show encryption status, and authentication mechanism for all connections from ABD 7) All of the above should address external services at the CSP/CSO level 8) When the external service is authorized, used the name from the FedRAMP Marketplace 9) When leveraging CSOs where FedRAMP authorization is conducted at the internal service level: a) This is typical for FedRAMP Authorized IaaS/PaaS CSOs b) Depict on the ABD all the internal leveraged services in use c) Indicate the FedRAMP authorization status for each
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)	----	*For SC-20, the CSP should describe how DNS requests from outside the boundary to the CSP's authoritative servers receive DNSSEC compliant responses.* *For SC-21, the CSP should describe how DNS requests from inside the boundary for destinations outside the boundary receive DNSSEC compliant responses.*
16	Does the CSO adequately employ Domain-based Message Authentication, Reporting & Conformance (DMARC) requirements according to DHS BOD 18-01?	----	*If email is sent, on behalf of the government as part of the CSO, then DMARC must be implemented on the sending domain.*
Other Comments:			

Section D: Low SSP Critical Control Checks

Control	Control	OK/Concern	Comments
AC-2	Account Management	----	
AC-17	Remote Access	----	
CA-1	Certification, Authorization, Security Assessment Policy and Procedures	----	
CM-6	Configuration Settings	----	
CP-9	Information System Backup	----	
IA-2(1)	User Identification and Authentication (Organizational Users) - Network Access to Privileged Accounts	----	
IA-8(1)	Identification and Authentication (Non-Organizational Users)	----	
IR-8	Incident Response Plan	----	
RA-5	Vulnerability Scanning	----	
SC-7	Boundary Protection	----	
SC-13	Use of Cryptography - FIPS-validated or NSA-approved	----	
Other Comments:			

Section E: SAP Checks

#	Description	OK/Concern	Comments
1	FedRAMP SAP template used, including all sections?	----	
2	Security Test Case Procedures (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/Concern	Comments
1	FedRAMP SAR template used, including all sections?	----	
2	Are risks documented?	----	
2a	Have all external services been appropriately documented in the SAR?	----	*It is expected that the 3PAO accurately reflect the risks due to external service interconnections to the system. At minimum, there should be a correlation to the SSP.*
3	Was evidence provided, or was there a statement that evidence can be provided upon request?	----	
4a	Completed Security Test Case Procedures (Test Case Workbook) present and in accordance with the 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 Penetration 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 the number and comments.	----	
10	Are the numbers of risks/findings consistently stated within the SAR, where appropriate?	----	
11	Are the inventory tables in the SAR consistent with the SSP inventory?	----	
12	Are SAR test results consistent with FedRAMP Timeliness and Accuracy of Testing Requirements?	----	*Pen Test: ~* *Vuln Scanning: ~* *Controls Testing: ~*
Other Comments:			

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

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

#	Description	OK/Concern	Comments
1	Is the POA&M in the FedRAMP POA&M template?	----	
2	Is the POA&M consistent with the 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 the 3PAO? (Included in the SAR)	----	
4b	Have all ORs risks been accepted by the authorizing agency?	TBD	*Have all POA&M-listed ORs, that are not included in the SAR, been risk accepted by the authorizing agency? [Agency to advise during Review Meeting]*
5	Does the POA&M reflect adherence to FedRAMP time-frame requirements (completion dates by 30 days for High, 90 days for Moderate, and 180 days for Low vulnerabilities)?	----	

Other Comments:

v4.4

Controlled Unclassified Information

DRAFT - Agency Authorization Review Report - DRAFT

FR Package ID#

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

Key: Concern = Action may be required. OK = No action required. N/A = Not applicable for this package.

Section B: Documents Provided Check

#	Description	OK/Concern	#	Description	OK/Concern
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 and 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 Worksheet	----
3.4	Att. 4: Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)	----
3.5	Att. 5: Rules of Behavior (ROB)	----
3.6	Att. 6: Information System Contingency Plan (ISCP)	----
3.7	Att. 7: Configuration Management Plan (CMP)	----
3.8	Att. 8: Incident Response Plan (IRP)	----
3.9	Att. 9: Control Implementation Summary (CIS) Workbook	----
3.10	Att. 10: Federal Information Processing Standard (FIPS) 199 Categorization	----
3.11	Att. 11: Separation of Duties Matrix	----
3.12	Att. 12: FedRAMP Laws and Regulations	----
3.13	Att. 13: FedRAMP Integrated Inventory Workbook	----
5.1	App. A - Risk Exposure Table	----
5.2	App. B - Security Test Case Procedures	----
5.3	App. C - Infrastructure Scan Results	----
5.4	App. D - Database Scan Results	----
5.5	App. E - Web Application Scan Results	----
5.6	App. F - Assessment Results	----
5.7	App. G - Manual Test Results	----
5.8	App. H - Documentation Review Findings	----
5.9	App. I - Auxiliary Documents	----
5.10	App. J - Penetration Test Report	----
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/Concern	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 Worksheet tabs, as well as the SSP controls (by checkbox selected and in the implementation description)? Are the CIS/CRM and SSP controls consistent for customer responsibilities? A sampling of seven 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*
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?	----	
8a	Is the authorization boundary explicitly identified in the network diagram?	----	An acceptable boundary diagram is a clearly marked boundary (e.g., a labeled box or line around the components included). The diagram must be legible and readable. The diagram should: • Include a clearly defined authorization boundary, • Include system interconnections used to operate and support the intended mission/business functions, • Depict every tool, service, or component that is mentioned in the SSP narrative, and controls, • Identify those depicted tools, services, or components as either external or internal to the boundary, • Identify all interconnected systems, and whether they are FedRAMP Authorized (or not), • Depict how CSP and customer/agency access the service (e.g., authentication used to access service), • Depict all major software/virtual components (or groups of) within the boundary, • Be validated against the inventory, • Show alternate processing site, and • Show pulling of updates from external services, such as OS, and antivirus updates. Supporting text should describe all internal components.
8b	Does the CSO provide components to run on the client side?	----	
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 that includes all traffic flows for both internal and external users?	----	Data flow diagrams should be consistent with authorization boundary and: • Clearly identify anywhere federal data is to be processed, stored, or transmitted, • Clearly delineate how data comes into and out of the system boundary, • Clearly identify data flows for privileged, non-privileged and customers' access with MFA details, and • Depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed. • For each data flow, clearly depict protective mechanisms (encryption type and FIPS 140-2 validation or use of other alternative implementations such as physical protection via protective distribution systems [PDS]), where applicable. Note: If any data flows are not protected by encryption, the CSP should be prepared to provide the FedRAMP PMO clarifying details so that a risk decision can be made related to FedRAMP authorization: • Identify the data flow(s) and stores that is/are not encrypted, • Describe the impacted data (government data, government metadata, CSP data, etc.), • Sensitivity of the impacted data (Low vs Moderate), • Mitigations in place, • Remediation plan, where appropriate, • Projected date of remediation, where appropriate.
10	Does the CSP use any third-party or external cloud services that lack FedRAMP authorization? If so, please list them.	----	Check throughout the SSP for services specified and if they are in the boundary diagram. ID any services not called out as part of the boundary discussion/diagram.
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?	----	*Consistently address the external services referenced in C.10 and C.11a as follows:* *1) Table 8-3. Leveraged Authorizations - should contain all FedRAMP Authorized CSOs* *2) Tables 11-1. System Interconnections and 13-3. CA-3 Authorized Connections, and SAR Section 6. Risks Known For Interconnected Systems - should catalog all external services* *3) SA-9 External Information System Services - should address all external services where federal information is processed or stored* *4) Supporting narrative* *a) Provide a brief description of how each is used in support of the CSO* *b) Describe the data shared with each external service - particularly those lacking FedRAMP authorization* *5)) ABD* *a) Show how each external service interacts with users and the CSO boundary* *b) Depict the FedRAMP authorization status for each external service* *6) DFD - show encryption status, and authentication mechanism for all connections from ABD* *7) All of the above should address external services at the CSP/CSO level* *8) When the external service is authorized, used the name from the FedRAMP Marketplace* *9) When leveraging CSOs where FedRAMP authorization is conducted at the internal service level:* *a) This is typical for FedRAMP Authorized IaaS/PaaS CSOs* *b) Depict on the ABD all the internal leveraged services in use* *c) Indicate the FedRAMP authorization status for each*
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)	----	*For SC-20, the CSP should describe how DNS requests from outside the boundary to the CSP's authoritative servers receive DNSSEC compliant responses.* *For SC-21, the CSP should describe how DNS requests from inside the boundary for destinations outside the boundary receive DNSSEC compliant responses.*
16	Does the CSO adequately employ Domain-based Message Authentication, Reporting & Conformance (DMARC) requirements according to DHS BOD 18-01?	----	*If email is sent on behalf of the government as part of the CSO, then DMARC must be implemented on the sending domain.*

Other Comments:

Section D: Moderate SSP Control Checks

Control	Control	OK/Concern	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)	User Identification and Authentication (Organizational Users) - Network Access to Privileged Accounts	----	
IA-2(2)	User Identification and Authentication (Organizational Users) - for Network Access to Non-privileged Accounts	----	
IA-2(3)	User Identification and Authentication - Local Access to Privileged Accounts	----	
IA-2(11)	User Identification and Authentication - Remote Access - Separate Device Authentication	----	
IA-8(1)	Identification and Authentication (Non-Organizational Users)	----	
IR-8	Incident Response Plan	----	
RA-5	Vulnerability Scanning	----	
RA-5(5)	Vulnerability Scanning - Privileged Access Authorization	----	
RA-5(8)	Vulnerability Scanning - 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-8 and SC-8 (1)	Transmission Confidentiality and Integrity (internal and external)	----	
SC-13	Use of Cryptography - FIPS-validated or NSA-approved	----	
SC-28	Protection of Information at Rest	----	
Other Comments:			

Section E: SAP Checks

#	Description	OK/Concern	Comments
1	FedRAMP SAP template used, including all sections?	----	
2	Security Test Case Procedures (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/Concern	Comments
1	FedRAMP SAR template used, including all sections?	----	
2	Are risks documented?	----	
2a	Have all external services been appropriately documented in the SAR?	----	*It is expected that the 3PAO accurately reflect the risks due to external service interconnections to the system. At minimum, there should be a correlation to the SSP.*
3	Was evidence provided, or was there a statement that evidence can be provided upon request?	----	
4a	Completed Security Test Case Procedures (Test Case Workbook) present and in accordance with the 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 Penetration 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 the number and comments.	----	
10	Are the numbers of risks/findings consistently stated within the SAR, where appropriate?	----	
11	Are the inventory tables in the SAR consistent with the SSP inventory?	----	
12	Are SAR test results consistent with FedRAMP Timeliness and Accuracy of Testing Requirements?	----	*Pen Test: ~* *Vuln Scanning: ~* *Controls Testing: ~*

Other Comments:

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

Section G: POA&M Checks

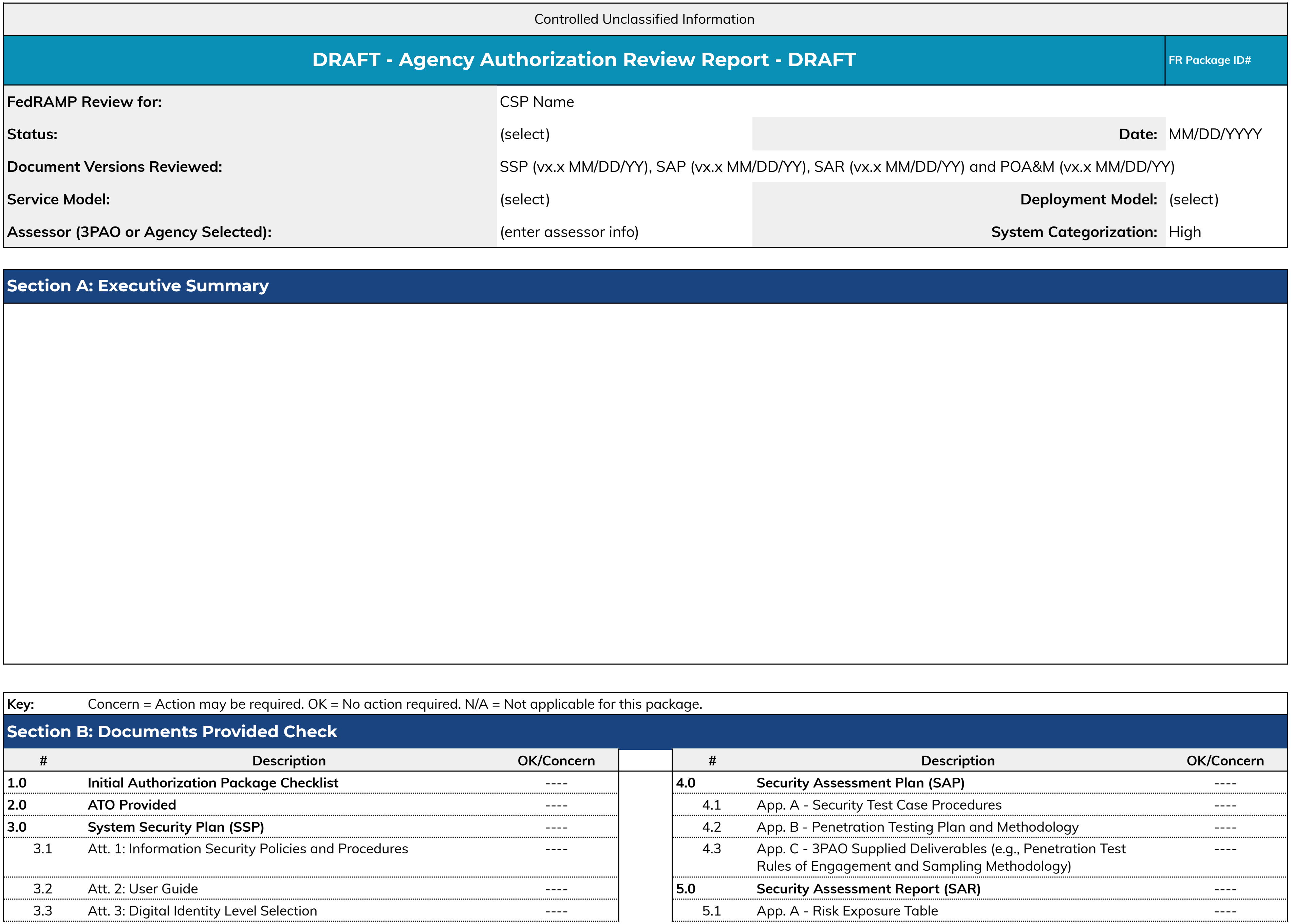
#	Description	OK/Concern	Comments

1	Is the POA&M in the FedRAMP POA&M template?	----	
2	Is the POA&M consistent with the 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 the 3PAO? (Included in the SAR)	----	
4b	Have all ORs risks been accepted by the authorizing agency?	TBD	*# of ORs not in SAR:* *Have all POA&M-listed ORs, that are not included in the SAR, been risk accepted by the authorizing agency? [Agency to advise during Review Meeting]*
5	Does the POA&M reflect adherence to FedRAMP time-frame requirements (completion dates by 30 days for High, 90 days for Moderate, and 180 days for Low vulnerabilities)?	----	

Other Comments:

# of ORs
# of VDs

v4.8



Controlled Unclassified Information

DRAFT - Agency Authorization Review Report - DRAFT

FR Package ID#

FedRAMP Review for:	CSP Name		
Status:	(select)	**Date:**	MM/DD/YYYY
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)		
Service Model:	(select)	**Deployment Model:**	(select)
Assessor (3PAO or Agency Selected):	(enter assessor info)	**System Categorization:**	High

Section A: Executive Summary

Key: Concern = Action may be required. OK = No action required. N/A = Not applicable for this package.

Section B: Documents Provided Check

#	Description	OK/Concern	#	Description	OK/Concern
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 and 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: FedRAMP Laws and Regulations	----	5.10	App. J - Penetration Test Report	----
3.13	Att. 13: FedRAMP 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/Concern	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 Worksheet tabs, as well as the SSP controls (by checkbox selected and in the implementation description)? Are the CIS/CRM and SSP controls consistent for customer responsibilities? A sampling of seven 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*
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	Was Digital Identity Level 3 selected and implemented, as required?	----	*Spot Check implementation status, parameters, and description for following associated controls:IA-8(2)/(3)/(4), IA-5, IA-5(3), SC-12(3). Also, reference related critical control concerns that reveal issues in (IA-2 (11) and IA- 2(12)).*
8a	Is the authorization boundary explicitly identified in the network diagram and are all associated services appropriately included within the boundary?	----	*An acceptable boundary diagram is a clearly marked boundary (e.g., a labeled box or line around the components included). The diagram must be legible and readable.* *The diagram should:* *• Include a clearly defined authorization boundary,* *• Include system interconnections used to operate and support the intended mission/business functions,* *• Depict every tool, service, or component that is mentioned in the SSP narrative, and controls,* *• Identify those depicted tools, services, or components as either external or internal to the boundary,* *• Identify all interconnected systems, and whether they are FedRAMP Authorized (or not),* *• Depict how CSP and customer/agency access the service (e.g., authentication used to access service),* *• Depict all major software/virtual components (or groups of) within the boundary,* *• Be validated against the inventory,* *• Show alternate processing site, and* *• Show pulling of updates from external services, such as OS, and antivirus updates.* *Supporting text should describe all internal components.*
8b	Does the CSO provide components to run on the client side?	----	
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 that includes all traffic flows for both internal and external users?	----	*Data flow diagrams should be consistent with authorization boundary and:* *• Clearly identify anywhere federal data is to be processed, stored, or transmitted,* *• Clearly delineate how data comes into and out of the system boundary,* *• Clearly identify data flows for privileged, non-privileged and customers' access with MFA details, and* *• Depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed.* *• For each data flow, clearly depict protective mechanisms (encryption type and FIPS 140-2 validation or use of other alternative implementations such as physical protection via protective distribution systems [PDS]), where applicable.* *Note: If any data flows are not protected by encryption, the CSP should be prepared to provide the FedRAMP PMO clarifying details so that a risk decision can be made related to FedRAMP authorization:* *• Identify the data flow(s) and stores that is/are not encrypted,* *• Describe the impacted data (government data, government metadata, CSP data, etc.),* *• Sensitivity of the impacted data (Low vs Moderate),* *• Mitigations in place,* *• Remediation plan, where appropriate,* *• Projected date of remediation, where appropriate.*
10a	Are any third-party or external cloud services lacking FedRAMP authorization used?	----	*Check throughout SSP for Services specified and if in boundary diagram. ID any services not called out as part of Boundary discussion/diagram.*
10b	Are all interconnections correctly identified and documented in the SSP?	----	

11a	If this is a SaaS or a PaaS, is it "leveraging" another IaaS with a FedRAMP authorization?	----	
11b	If 11a is Yes, is the leveraged service a High service?	----	
11c	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?	----	*Consistently address the external services referenced in C.10 and C.11a as follows:* *1) Table 8-3. Leveraged Authorizations - should contain all FedRAMP authorized CSOs* *2) Tables 11-1. System Interconnections and 13-3. CA-3 Authorized Connections, and SAR Section 6. Risks Known For Interconnected Systems - should catalog all external services* *3) SA-9 External Information System Services - should address all external services where federal information is processed or stored* *4) Supporting narrative* *a) Provide a brief description of how each is used in support of the CSO* *b) Describe the data shared with each external service - particularly those lacking FedRAMP authorization* *5)) ABD* *a) Show how each external service interacts with users and the CSO boundary* *b) Depict the FedRAMP authorization status for each external service* *6) DFD - show encryption status, and authentication mechanism for all connections from ABD* *7) All of the above should address external services at the CSP/CSO level* *8) When the external service is authorized, used the name from the FedRAMP Marketplace* *9) When leveraging CSOs where FedRAMP authorization is conducted at the internal service level:* *a) This is typical for FedRAMP authorized IaaS/PaaS CSOs* *b) Depict on the ABD all the internal leveraged services in use* *c) Indicate the FedRAMP authorization status for each*
13	Are all required controls present?	----	
14	Are controls requiring automation implemented, where required?	----	Review of following controls: - AC-2(1), AC-12, AC-18 (03) - AU-6(1), AU-03 (02), AU-06 (04), AU-07 (01) - AT-03 (04) - CA-07 - CM-2(2), CM-3(1), CM-03 (06), CM-6(1), CM-8(3), CM-8(2), CM-11 - CP-10 - IR-4(1), IR-5(1), IR-6(1) - PE-03, PE-8(1), PE-11 (01), PE-13(1), PE-13 (2), PE-13 (3), PE-15(1) - PS-4(2) - SC-23 (01) - SI-2(2), SI-03 (02), SI-4(2), SI-04 (20), SI-5(1), SI-7(2), SI-7(5), SI-08 (02)
15	Are technical controls implemented?	----	Review of following controls: - AC-02 (10),AC-03 ,AC-05, AC-06 ,AC-06 (01),AC-06 (05),AC-06 (07),AC-06 (09),AC-06 (10), AC-07, AC-07 (02),AC-08,AC-10,AC-11, AC-11 (01), AC-12, AC-17 (01),AC-17 (02), AC-18 (01), AC-19, AC-19 (5), AC-20, AC-20 (01), AC-20 (02), AC-21 - AU-02 (03), AU-05 (02), AU-06, AU-06 (07), AU-07 (01), AU-09 (02), AU-09 (04), AU-11 - CM-05, CM-05 (01), CM-10 - IA-04 (04), IA-05 (04), IA-06 - IR-02 (02) - SC-07 (05), SC-10
16	Is the inventory provided in the FedRAMP Inventory Workbook?	----	

17	Is the CSO compliant with DNSSEC? (Controls SC-20 and SC-21 apply)	----	*For SC-20, the CSP should describe how DNS requests from outside the boundary to the CSP's authoritative servers receive DNSSEC compliant responses.* *For SC-21, the CSP should describe how DNS requests from inside the boundary for destinations outside the boundary receive DNSSEC compliant responses.*
18	Does the CSO adequately employ Domain-based Message Authentication, Reporting & Conformance (DMARC) requirements according to DHS BOD 18-01?	----	*If email is sent on behalf of the government as part of the CSO, then DMARC must be implemented on the sending domain.*
Other Comments:			

Section D: High SSP Control Checks

Control	Control	OK/Concern	Comments
AC-2	Account Management	----	*Also check HBL control enhancements for AC-2, noting any concerns, for following: AC-2(2)/(3)/(4)/(5)/(7)/(9)/(11)/(12)/(13)*
AC-4	Information Flow Enforcement	----	
AC-17	Remote Access	----	*Also check AC-17(09) FedRAMP Parameter implementation*
AC-18	Wireless Access Restrictions	----	*Also check AC-19 and AC-19 (5)*
AU-12(1)	Audit Generation	----	*FedRAMP Parameter -- The information system compiles audit records from [FedRAMP Assignment: all network, data storage, and computing devices] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].*
CA-1	Security Assessment and Authorization Policies and Procedures	----	*Also ensure FedRAMP HBL Parameters are addressed (at least annually &/or for a significant change)*
CM-6	Configuration Settings	----	*Also check Control Enhancement CM-6 (2)*
CM-11(1)	User-Installed Software - Alerts for Unauthorized Installation	----	
CP-7	Alternate Processing Site	----	*Also check control enhancement CP-7(4)*
CP-8(3)	Telecom. Services - Separated Alternate Telecom. Services	----	
CP-9	Information System Backup	----	*Also check CEs and FR Parameters for CP-9(1)/(2)/(5)*
IA-2(1)	User Identification and Authentication (Organizational Users) - Network Access to Privileged Accounts.	----	
IA-2(2)	User Identification and Authentication (Organizational Users) - for Network Access to Non-privileged Accounts	----	
IA-2(3)	User Identification and Authentication - Local Access to Privileged Accounts	----	*Not required in all instances; for example, SaaS CSPs may be N/A; IaaS may use alternative implementation*

IA-2(4)	User Identification and Authentication - Local Access to Non-privileged Accounts	----	
IA-2(9)	User Identification and Authentication - network access to Non-privileged Accounts - Replay-resistant	----	
IA-2(11)	User Identification and Authentication - Remote Access - Separate Device Authentication	----	
IA-2(12)	User Identification and Authentication - Acceptance of PIV Credentials	----	
IA-5	Authenticator Management	----	
IA-8(1)	Identification and Authentication (Non-Organizational Users)	----	
IR-8	Incident Response Plan	----	*Also check FR control enhancement IA-5(7)*
RA-5	Vulnerability Scanning	----	
RA-5(4)	Vulnerability Scanning - Discoverable Info, Notification and Corrective Action	----	
RA-5(5)	Vulnerability Scanning - Privileged Access Authorization	----	
RA-5(6)	Vulnerability Scanning - Automated Mechanisms for Trends Determination	----	
RA-5(8)	Vulnerability Scanning - Review Historic Audit Logs	----	
RA-5(10)	Vulnerability Scanning - Correlation of Output for Presence of Multi-vulnerability/Multi-hop Attack Vectors	----	
SA-9(5)	System and Services Acq. - Ext. Info Sys. Processing, Storage, and Service Location	----	*FedRAMP Parameters require:* *SA-9 (5)-1 [information processing, information data, AND information services]* *SA-9 (5)-2 [US/US Territories or geographic locations where there is US jurisdiction]* *SA-9 (5)-3 [all High impact data, systems, or services]*
SA-11	Developer Security Testing and Evaluation	----	
SA-11(1)	Developer Security Testing and Evaluation - Static Code Analysis	----	*R3 requires a Code Analysis Report and that it be in a ConMon Plan*
SC-2	Application Partitioning	----	
SC-3	Secure Function Isolation	----	
SC-4	Information in Shared Resources	----	
SC-7	Boundary Protection	----	*Also check following CEs for FR HBL control or parameter implementation: SC-7(4)/(10)/(12)/(13)/(20)/(21)*
SC-8 and SC-8 (1)	Transmission Confidentiality and Integrity	----	
SC-12(1)	Cryptographic Key Establishment & Management - Availability	----	
SC-13	Cryptographic Protection - FIPS-validated or NSA-approved	----	*Also check SC-8, SC-8(1), and SC-28 for consistency*
SC-28	Protection of Information at Rest	----	
SI-4(11)	Info System Monitoring - Analyze Comms. Traffic, Anomalies	----	
SI-4 (18)	Info System Monitoring - Outbound Traffic, Covert Exfiltration	----	
Other Comments:			

Section E: SAP Checks

#	Description	OK/Concern	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/Concern	Comments
1	FedRAMP SAR template used, including all sections?	----	
2	Are risks documented?	----	
2a	Have all external services been appropriately documented in the SAR?	----	*It is expected that the 3PAO accurately reflect the risks due to external service interconnections to the system. At minimum, there should be a correlation to the SSP.*
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 the 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 Penetration 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 the 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?	----	*Pen Test: ~* *Vuln Scanning: ~* *Controls Testing: ~*
Other Comments:			
Findings: *High:* *Mod:* *Low:* *# of risks downgraded (by level) due to mitigating factors* *# of ORs*			

Section G: POA&M Checks

#	Description	OK/Concern	Comments
1	Is the POA&M in the FedRAMP POA&M template?	----	
2	Is the 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 the 3PAO? (Included in the SAR)	----	
4b	Have all ORs risks been accepted by the authorizing agency?	TBD	*Have all POA&M-listed ORs, that are not included in the SAR, been risk accepted by the authorizing agency? [Agency to advise during Review Meeting]*
5	Does the POA&M reflect adherence to FedRAMP time-frame requirements (completion dates by 30 days for High, 90 days for Moderate, and 180 days for Low vulnerabilities)?	----	
Other Comments:			