OMB Control #: 0938-NEW
Expiration Date: XX/XX/20XX

Sensitive and Confidential Information – For Official Use Only

Non-Exchange Entity Name (Acronym)

Security and Privacy Assessment Report of the <Name of Non-Exchange Entity>

<Name of NEE Information System>

As performed by <Auditor Company Name>

SAR Version 0.1

Report Publication Date

CMS SAR Template v 3.2

Security and Privacy Assessment Report

Prepared by: <Identify Independent Third-Party Auditor that prepared this document>

Organization Name: <Enter Company/Organization>.

Street Address: <Enter Street Address>

Suite/Room/ Building: <Enter Suite/Room/Building>

City, State Zip: <Enter Zip Code>

Prepared for: <Identify Non-Exchange Entity>

Organization Name: <Enter Company/Organization>.

Street Address: <Enter Street Address>

Suite/Room/ Building: <Enter Suite/Room/Building>

City, State Zip: <Enter Zip Code>

Revision History

Date	Description	Version of SAR	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

Table of Contents

List of Tables

1. Executive Summary

The primary purpose of this document is to provide a Security and Privacy Assessment Report (SAR) for <NEE> for the purpose of making risk-based decisions.

A Security and Privacy Assessment of <NEE> was conducted between <mm/dd/yyyy – mm/dd/yyyy>. The assessment was conducted in accordance with the approved Security and Privacy Assessment Plan (SAP), dated <SAP Date>, <SAP Version #>.

Table 1 represents the aggregate risks identified from the assessment. This table should reflect all findings reported in the Detailed Findings Table.

Table 1. Executive Summary of Risks

Risk Category	Number of Risks
Critical	0
High	0
Moderate	0
Low	0
Total Risks	**0**

2. Introduction and Purpose

The Patient Protection and Affordable Care Act (ACA) program requires a Non-Exchange Entity (NEE) to use an independent third-party Auditor to perform security and privacy assessment testing and to develop a Security and Privacy Assessment Report (SAR) based on the outcomes of the assessment. Enhanced Direct Enrollment (EDE) Entities are considered NEEs. The < Auditor Name> performed security and privacy testing for <Information System Abbreviation> in accordance with the <Information System Abbreviation> Security and Privacy Controls Assessment Test Plan (SAP), <SAP Date>, <SAP Version #>.

This SAR provides the <NEE> ISSO, SOP, and the AOs with the results of the assessment completed for the <Information System Abbreviation>. The SAR describes risks associated with the vulnerabilities identified during the <Information System Abbreviation> independent security and privacy assessment and serves as the risk summary report as referenced in the *Framework for Independent Assessment of Security and Privacy Controls for NEEs Entities* and NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

2.1 Applicable Laws, Regulations, and Standards

By interconnecting with the CMS network and the CMS information system, the EDE Entity agrees to be bound by the EDE Interconnection Security Agreement (ISA) and the use of the

CMS network and information system in compliance with the ISA. Concurrently, by interconnecting with the CMS network and the CMS information system, NEEs that are participating in the classic Direct Enrollment program only (e.g., Web-Brokers not participating in the EDE program), agree to be bound by the terms of *Agreement between Web-Broker and CMS for the Federally-Facilitated Exchanges and State-Based Exchanges on the Federal Platform.* The following applicable laws, regulations, and standards apply (the NEE may also add state laws, regulations, and standards as applicable):

- Federal Information Security Management Act of 2014 (FISMA)
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
- 18 U.S.C. § 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information
- Privacy Act of 1974, 5 U.S.C. § 552a
- Health Insurance Portability and Accountability Act (HIPAA) of 1966 (P.L. 104-191)
- Patient Protection and Affordability Care Act of 2010
- HHS Regulation, 45 CFR § 155.260 – Privacy and Security of Personally Identifiable Information
- HHS Regulation, 45 CFR § 155.280 – Oversight and monitoring of privacy and security requirements
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*

2.2 Scope

The Auditor analyzed all assessment results to provide the <NEE> Information System Security Officer (ISSO), Senior Official for Privacy (SOP), and the Authorizing Officials (AO) with an assessment of the security and privacy controls that safeguard the confidentiality, integrity, and availability (CIA) of data hosted by the system as described in the <Information System Abbreviation> System Security and Privacy Plan (SSP).

This document consists of a SAR for <Information System Name> <Information System Abbreviation> as required by <*Insert reason for the assessment*>. This SAR presents the results of a security and privacy test and evaluation of the <Information System Abbreviation> and is provided to support the <NEE> <Acronym of NEE> program goals, efforts, and activities necessary to achieve compliance with the necessary security and privacy requirements.

The <NEE> engaged < Auditor Name > to perform an onsite security and privacy controls assessment (SCA) of the <Information System Name> to determine:

- If the system is in compliance with the CMS security and privacy standards described in the EDE SSP;
- If the underlying infrastructure supporting the system is secure;

- If the system and data are securely maintained; and
- If proper configuration associated with the database and file structure storing the data are in place.

The SCA consisted of system components and documentation reviews. The following components were tested during this assessment:

> **Instruction:** Provide a list of components (e.g., hardware, software, etc.) that were planned to be tested and those that were actually tested during the assessment. These components may be items identified in the SAP, Section 2. Include additional documents as necessary.
>
> - Example: Operating system(s): Windows, Linux and version
> - Example: Database and version #
> - Example: Information System, and sub-components
> - Example: Web Applications and URLs
>
> Security and privacy documentation will be reviewed for completeness and accuracy Through this process, the Auditor will gain insight to determine if all controls are implemented as described. The Auditor's review also augments technical control testing.
>
> The Auditor must review, at a minimum, the following required documents for assessment Additional documents or supporting artifacts may be reviewed as necessary. Please ensure the document file name includes version number and date (e.g. Configuration Management Plan v2.2 07/21/2022).
>
> [Delete this and all other instructions from your final version of this document.]

The following documents will be assessed:

- Business Agreement with Data Use Agreement (DUA);
- Configuration Management Plan (CMP);
- Contingency Plan (CP) and Test Results;
- Plan of Action and Milestones (POA&M);
- System Security and Privacy Plan (SSP) Final;
- Incident Response Plan (IRP) and Incident/Breach Notification and Test Plan;
- Privacy Impact Assessment (PIA) and other privacy documentation, including, but not limited to, privacy notices as well as agreements to collect, use, and disclose Personally Identifiable Information (PII) and Privacy Act Statements;
- Security Awareness Training (SAT) Plan and Training Records;
- Interconnection Security Agreements (ISA);
- Information Security Risk Assessment (ISRA);
- Governance documents and privacy policy; and

- Documentation describing the organization's privacy risk assessment process and documentation of privacy risk assessments performed by the organization.

The assessor interviewed business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. Interviews were customized to focus on control assessment procedures that apply to individual roles and responsibilities and assure proper implementation and/or execution of security and privacy controls.

Table 2 describes the personnel selected to be interviewed and their respective roles.

Table 2. Personnel Interviews

Title	Name of Person	Date of Interview	Comments
Business Owner(s)	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Application Developer	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Configuration Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Contingency Planning Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Database Administrator	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Data Center Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Facilities Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Firewall Administrator	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Human Resources Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Information System Security Officer	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Privacy Program Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Privacy Officer	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]

Title	Name of Person	Date of Interview	Comments
Media Custodian	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Network Administrator	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Program Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
System Administrators	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
System Owner	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Training Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]

3. System Overview

3.1 System Description

Instruction: In this subsection, insert a general description of the information system. The description should be consistent with the description found in the SSP. The description in this subsection may differ only if additional information is included that is not available in the SSP or if the description in the SSP is not accurate.

[Delete this instruction and all other instructions from your final version of this document.]

[Click **here** and type text.]

3.2 Purpose of System

Instruction: Insert the purpose of the information system. The purpose must be consistent with the SSP.

[Delete this instruction and all other instructions from your final version of this document.]

[Click **here** and type text.]

4. Summary Report

The Auditor has complied with the terms articulated in the SAP and the assessment is complete and comprehensive. Appendices A through C provides the infrastructure, database, web application scan results. Appendix D provides the penetration test report which includes test results for all components within scope of the information system. Appendix E provides the summary results of all scans.

4.1 Summary of Findings

Instruction: Provide a narrative summary of the findings relating to the security and privacy control families. Complete the summary findings Table 3 for ALL findings from the assessment regardless type of test.

The Auditor must provide a total of number system risks that were identified for the information system. The Auditor must identify the number of High risks, Moderate risks, and Low risks for all findings, including but not limited to, scan results, penetration test results, interviews, and control test results. Priority levels are based on the type of vulnerability identified.

Examples of findings fall into the following areas:

- Access Control: An access control addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Account Management: Review information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
- Application Security: Enforces approved authorizations for logical access to information and system resources.
- Auditing and Monitoring: The organization monitors for evidence of unauthorized disclosure of organizational information.
- Configuration Management: Describes how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents.
- Database Management: Determines the types of changes to the database that are configuration-controlled.
- Documentation Updates: Addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements.
- Identification and Authentication: The information system uniquely identifies and authenticates organizational users.

- Security Management: Verifies the identity of the individual, group, role, or device receiving the authenticator.
- Software Maintenance: Uses software and associated documentation in accordance with contract agreements and copyright laws.
- System and Information Integrity: Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Authority and Purpose: Determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.
- Accountability, Audit, and Risk Management: The organization has a designated privacy official who is accountable for developing, implementing, and maintaining governance and a strategic privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems.
- Data Quality and Integrity: The organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API).
- Data Minimization and Retention: The organization identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.
- Individual Participation and Redress: The organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection.
- Security: The organization establishes, maintains, and updates, within every 365 days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.
- Transparency: Provides effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization.
- Use Limitation: The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
- If N/A is provided, please provide a detailed explanation as to why.

[Delete this instruction and all other instructions from your final version of this document.]

Table 3. Summary Findings Table

Row #	Weakness	Risk Level	Control #	POA&M Reference #

4.2 Summary of Recommendations

For each finding, the Auditor developed detailed recommendations for improvements that address the findings and the business and system risks. Most of the recommendations in this document fall into the following areas:

Instruction: While all findings must be addressed, findings representing a high business risk should be mitigated or closed immediately to reduce the risk exposure. The following example list of findings areas should be modified based on the SCA results:

- Block Unused Ports and Protocols:
- Perform Security and Privacy Monitoring:
- Strengthen Database Access Controls:
- Update Documentation:

  Provide a summary of recommendations grouped by families, if possible. Identify which corrective actions can mitigate large groups of findings.

  For example: The Access Control (AC) and most of the Configuration Management (CM) findings can be remediated if the database is upgraded to the latest version of the software, and necessary hot fixes and patches are applied.

[Delete this instruction and all other instructions from your final version of this document.]

[Click **here** and type text.]

5. Detailed Findings Report

Instruction: Provide a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Include findings from all scans and tests. For each vulnerability, provide the following:

- Explanation of the vulnerability
- Identification of specific risks to the continued operations of the system

- Analysis of impact of each risk
- Suggested corrective actions for closing or reducing the impact of each vulnerability

Auditors must test for the Concurrent Session Control and Remote Access use cases as documented in the EDE Auditor Guidelines and document results in Table 4.

- **Concurrent Session Control:** The information system must prohibit agent/broker use of concurrent sessions by FFE user ID.
  Review Standard: The Auditor must validate the EDE Entity is able to effectively block the creation of an additional account where the account creation is attempted using the same FFE User ID; and that the EDE environment effectively prohibits concurrent sessions.

- **Remote Access: Access** to the FFEs and SBE-FPs. EDE Entity and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through VPN.
  Review Standard: The Auditor must validate and document in the SAR that existence of automated mechanisms to monitor and control remote access methods. The Auditor must verify automated mechanism block IP addresses located outside of the United States of America or its territories, embassies, or military installations attempting to access the EDE environment.

[Delete this instruction and all other instructions from your final version of this document.]

Table 4 provides a summary of the assessment results by control family. Progress on satisfying any previously identified weaknesses must be actively monitored. Details of this review including any management comments are provided in the <Information System Name> Security and Privacy Assessment Worksheet.

Instruction: Add the numbers in Table 4.

SAMPLE Assessment Results

Security Controls	Total Controls	Met	Partially Met	Not Met
AC – Access Control	6	2	3	1
Concurrent Session Testing: AC-2: Account Management	1	1		
Concurrent Session Testing: AC-10 Concurrent Session Control	1		1	

Security Controls	Total Controls	Met	Partially Met	Not Met
Remote Access Testing: AC-17: Remote Access	1			1
AT – Awareness and Training	4	2	1	1
AU – Audit and Accountability	7	3	2	2

[Delete this instruction, including the foregoing table, and all other instructions from your final version of this document.]

Table 4. Assessment Results

Security Controls	Total Controls	Met	Partially Met	Not Met
AC – Access Control				
Concurrent Session Testing: AC-2: Account Management				
Concurrent Session Testing: AC-10 Concurrent Session Control				
Remote Access Testing: AC-17: Remote Access				
AT – Awareness and Training				
AU – Audit and Accountability				
CA – Security Assessment and Authorization				
CM – Configuration Management				
CP – Contingency Planning				
IA – Identification and Authentication				
IR – Incident Response				
MA – Maintenance				
MP – Media Protection				
PE – Physical and Environmental Protection				
PL – Planning				
PM – Program Management				
PS – Personnel Security				
RA – Risk Assessment				
SA – System and Services Acquisition				
SC – System and Communications Protection				
SI – System and Information Integrity				

Security Controls	Total Controls	Met	Partially Met	Not Met
AP – Authority and Purpose				
AR – Accountability, Audit, and Risk Management				
DI – Data Quality				
DM – Data Minimization and Retention				
IP – Individual Participation and Redress				
SE – Security				
TR – Transparency				
UL – Use Limitation				
TOTAL CONTROLS				

5.1 Detailed Findings Table

Instructions: This subsection provides a description of the columns in the Detailed Findings Table (Table 5).

Row Number

Each finding has a row number included to provide easy reference for briefings and cross-referencing.

POA&M Reference

Verify that the findings are identified in the Plan of Action and Milestones (POA&M).

Weakness

The Weakness column provides a brief description of the security and privacy vulnerability.

Risk Level

Each finding is considered a business risk and assigned a risk level rating of high, moderate, or low. The rating provides an assessment of the magnitude of the finding and helps establish a priority for addressing the vulnerability. The following table defines the Risk levels.[1]

[1] These risk levels are aligned NIST SP 800-30 Rev. 1.

Definition of Risk Levels

Rating	Definition of Risk Rating
Critical	A threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, or other organizations.
High	A threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, or other organizations.
Moderate	A threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, or other organizations.
Low	A threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, or other organizations.

Control Number

The Control Number column identifies the EDE security and privacy control family and control number that is affected by the vulnerability, for example, (AC)-1: Access Control.

Center for Internet Security (CIS) Top 18 Control

State whether the control falls under a CIS Top 18 control area.[2]

Open Web Application Security Project (OWASP) Top 10

State whether the finding falls under one of the OWASP Top 10 most critical web application security risks.[3]

Affected Systems

The systems, URLs, IP addresses, etc., affected by the weakness, are documented in the Affected Systems column. For example: SQL Server:master, or http://127.0.0.1

Finding

A detailed description of the finding provides information on how the actual test results fail to meet the security and privacy requirement. The first line of this description with the date of the SAR is used to prepare the Plan of Action and Milestone(s) and provides easy reference to the SAR for additional information.

Failed Test Description

The column for Failed Test Description documents the control's weakness that resulted in the finding. This description provides specific information from the security and privacy policy, requirements, guidance, test objective, or published industry best practices that was not provided with the controls implementation.

2 See https://www.cisecurity.org/controls/cis-controls-list/.

3 See https://owasp.org/www-project-top-ten/.

Actual Test Results

The Actual Test Results provide specific information on the observed failure of the test objective, policy, or guidance. This may also contain output from a test performed on the system revealing non-compliance.

Corrective Actions

The Corrective Actions column presents the recommended actions to resolve the vulnerability. The Auditor provides these suggestions to present guidance on a potential fix.

POA&M Reference

Identify the corresponding POA&M reference number. All findings listed must have a POA&M reference number or state if the finding was remediated during the assessment.

Status

The Status column provides status information, which includes when the vulnerability was identified, actions being taken, or resolution of the weakness or vulnerability.

If N/A is provided for any column, please provide a detailed explanation as to why.

[Delete this instruction and all other instructions from your final version of this document.]

Complete Table 5, Table 6, and Table 7. For Table 5, please complete the standalone Excel file entitled, "Detailed Findings Table_SAR Template," to input findings.

Table 5. Detailed Findings Table

Table 6. Summary of CIS Top 18 Controls

Assessment Results	Count
Partially Met	0
Not Met	0
TOTAL	0

Table 7. Summary of OWASP Top 10

Assessment Results	Count
Partially Met	0
Not Met	0
TOTAL	0

Appendix A. Infrastructure Scan Results

Infrastructure scans include scans of operating systems, networks, routers, firewalls, domain name servers (DNS), domain servers, network information security (NIS) masters, and other devices that keep the network running. These scans can include both physical and virtual Host and devices. The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Abbreviation> infrastructure. <Number> percent of the inventory was scanned. For the remaining inventory, the Auditor performed a manual review of configuration files to analyze for existing vulnerabilities. Any findings found as the result of the scans were documented in the SAR's Detailed Findings Table (Table 5).

A.1 Infrastructure Scans: Raw Scan Results

Instruction: Provide all - 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.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 8 lists the files that are included.

Table 8. Raw Scan Results by Infrastructure Scanner

Title of the Document	Description	File Name (Includes Extension)

A.2 Infrastructure Scans: Total Findings Discovered

Instruction: Summarize the Infrastructure scan assessment results in the following table. Ensure that the scanner severity level is appropriately mapped to the risk level ratings.

The number of reported findings from the scan results should match the combined number of findings in Table 9 and Table 10.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 9. Findings Discovered by Infrastructure Scanner

Risk Level	Infrastructure Scans
Critical	
High	
Moderate	
Low	
Total	

A.3 Infrastructure Scans: False Positive Reports

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.]

Table 10 identifies false positives that were generated by the infrastructure scanner.

Table 10. False Positive Reports by Infrastructure Scanner

ID #	Page and IP Address	Scanner Severity Level	Finding	False Positive Explanation
1-FP-IS				
2-FP-IS				

Appendix B. Database Scan Results

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Abbreviation> databases. <Number> % percent of all databases were scanned.

B.1 Database Scans: Inventory of Databases Scanned

Instruction: Indicate the databases that were scanned. 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.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 11 presents the database inventory scan results.

Table 11. Database Inventory Scan Results

IP Address	Hostname	Software / Version	Function	Comment

B.2 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.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 12 lists the files that are included.

Table 12. Raw Scan Results

Title of Document	Description	File Name (Includes Extension)

Title of Document	Description	File Name (Includes Extension)

B.3 Database Scans: Findings Discovered

Instruction: Summarize the Database scan assessment results in the following table. Ensure that the scanner severity level is appropriately mapped to the risk level ratings.

The number of reported findings from the scan results should match the combined number of findings in Table 13 and Table 14.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 13. Findings Discovered by Database Scanner

Risk Level	Database Scans
Critical	
High	
Moderate	
Low	
Total:	

B.4 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 14 identifies false positives that were generated by the database scanner.

Table 14. False Positives Generated by the Database Scanner

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

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

Appendix C. Web Application Scan Results

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Abbreviation> web applications. <Number> % of all web applications was scanned.

Instruction: Indicate the web applications that were scanned. For "Function," indicate the function that the web-facing application plays for the system (e.g., control panel to build virtual machines). Add additional rows as necessary.

If N/A is provided, please provide a detailed explanation as to why.

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

C.1 Web Applications Scans: Inventory of Web Applications Scanned

Table 15 lists the web applications that were scanned and the function that the web-application performs for the system.

Table 15. Inventory of Web Applications Scanned

Login URL	IP Address of Login Host	Function	Comment

C.2 Web Applications Scans: Raw Scan Results

Instruction: Provide all web application scans 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.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 16 lists the files that are included.

Table 16. Raw Scan Results

Title of Document	Description	File Name (Includes Extension)

C.3 Web Application Scans: Findings Discovered

Instruction: Summarize the Web Application scan assessment results in the following table. Ensure that the scanner severity level is appropriately mapped to the risk level ratings.

The number of reported findings from the scan results should match the combined number of findings in Table 13 and Table 14.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 17. Findings Discovered by Web Application Scanner

Risk Level	Web Application Scans
Critical	
High	
Moderate	
Low	
Total:	

C.4 Web Applications 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 "WS" in the identifier number refers to "Web Application Scan."

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

Table 18 identifies each false positive that was generated by the web applications scanner.

Table 18. False Positive Reports by Web Applications Scanner

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

Appendix D. Penetration Test Report

Instruction: The results reported in this appendix should be components identified in Section 2 of the Security and Privacy Controls Assessment Test Plan and should include the OWASP Top 10 results specified in subsection 2.4.

If penetration test is completed by a separate assessment organization, the primary security assessment organization must complete all sections of the SAR.

If N/A is provided, please provide a detailed explanation as to why.

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

The scope of this assessment was limited to the <Information System Abbreviation> solution, including <List components here as documented in the Security and Privacy Test Plan Section 2 or > components. The Auditor conducted testing of <Acronym of EDE Entity> activities from the <Location > via an attributable Internet connection.

Table 19 provides IP addresses and uniform resource locators (URL) for all the in-scope systems at the beginning of the assessment.

Table 19. IP Addresses and URLs for In-Scope Systems

Application	IP/URL	OWASP Top 10	Penetration Test Results

D.1 Penetration Test Report: Findings Discovered

Instruction: Summarize the Penetration Test results in the following table. Ensure that the scanner severity level is appropriately mapped to the risk level ratings.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 20. Findings Discovered by Penetration Testing

Risk Level	Penetration Test Results
Critical	
High	
Moderate	
Low	

Risk Level	Penetration Test Results
Total:	

Appendix E. Penetration Test and Scan Results Summary

Instruction: Summarize the scan assessment results in the following table. Ensure that the scanner severity level is appropriately mapped to the risk level ratings.

If N/A is provided, please provide a detailed explanation as to why.

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

Table 21 is a summary of all scan assessment results appropriately mapped to the risk level ratings.

Table 21. Summary of Scan Results

Risk Level	Infrastructure Scans	Web Scans	DB Scans	Penetration Test	Total
Critical					
High					
Moderate					
Low					
Total					

Table 22 summarizes the total risk findings from penetration and scan testing.

Table 22. Total Risk Findings from Penetration and Scan Testing

Risk Level	Risks from Penetration and Scan Testing	Total Risks from Penetration and Scan Testing
Critical	<#>	<#> (<#>% of Grand Total)
High	<#>	<#> (<#>% of Grand Total)
Moderate	<#>	<#> (<#>% of Grand Total)
Low	<#>	<#> (<#>% of Grand Total)
Total	<#>	<#>