Centers for Medicare & Medicaid Services

Affordable Care Act (ACA) Health Insurance Administering Entity

**Administering Entity** Security and Privacy Assessment Report (SAR) for **[AE Name (Acronym) System Name (Acronym)]**

As performed by [Assessor Company Name]

Version **[#]**

Report Publication Date: [**MM DD, YYYY]**

Template v 1.1 dated 04 06, 2020

Security and Privacy Assessment Report

Prepared by: [Identify Independent Third-party assessor 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: [Administering 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> |

[Record of Template Changes: Delete table before use]

| **Version Number** | **Version Date** | **Author/ Owner** | **N=New**  **A=Add M=ModifyD=Delete** | **Description of Change** | **Substantive Change**  **[Y/N]** |
| --- | --- | --- | --- | --- | --- |
| [1.0 | 02/13/2019 | LL | N | Document creation. | --] |
| [1.1 | 04/06/2020 | LL | M | Changed Assessment worksheet name. Updated Appendix A. Minor grammar corrections and formatting changes. | N] |

[**General Instructions for Completing this Report:**

**IMPORTANT:** The State Administering Entity (AE) filling out the report should delete all bracketed instructions prior to either hardcopy or electronic distribution of the completed draft or final copy of the SAR.

Additionally, the AE should replace all bracketed text with the requested information and turn all blue text black.

Instructions for AEs are provided within the brackets [.…] in various locations throughout the document. Provide the required information, delete any remaining instructions and brackets, and normalize the font with the surrounding text before final submission.

Although the blank template is subject to no limitations on use or disclosure from CMS’ perspective, the completed template will contain sensitive proprietary information, and may only be disclosed as described under the terms of this SAR.]

Table of Contents

[1. Executive Summary 5](#_Toc37094581)

[2. Introduction and Purpose 5](#_Toc37094582)

[2.1 Applicable Laws, Regulations, and Standards 5](#_Toc37094583)

[2.2 Scope 6](#_Toc37094584)

[3. System Overview 9](#_Toc37094585)

[3.1 System Description 9](#_Toc37094586)

[3.2 Purpose of System 9](#_Toc37094587)

[4. Summary Report 9](#_Toc37094588)

[4.1 Summary of Findings 10](#_Toc37094589)

[4.2 Summary of Recommendations 12](#_Toc37094590)

[5. Detailed Findings Report 12](#_Toc37094591)

[5.1 Detailed Findings Table 14](#_Toc37094592)

[Appendix A. Security and Privacy Assessment Worksheet 18](#_Toc37094593)

[Appendix B. Infrastructure Scan Results 19](#_Toc37094594)

[B.1 Infrastructure Scans: Raw Scan Results 19](#_Toc37094595)

[B.2 Infrastructure Scans: False Positive Reports 19](#_Toc37094596)

[Appendix C. Database Scan Results 21](#_Toc37094597)

[C.1 Database Scans: Inventory of Databases Scanned 21](#_Toc37094598)

[C.2 Database Scans: Raw Scan Results 21](#_Toc37094599)

[C.3 Database Scans: False Positive Reports 22](#_Toc37094600)

[Appendix D. Web Application Scan Results 23](#_Toc37094601)

[D.1 Web Applications Scans: Inventory of Web Applications Scanned 23](#_Toc37094602)

[D.2 Web Applications Scans: Raw Scan Results 23](#_Toc37094603)

[D.3 Web Applications Scans: False Positive Reports 24](#_Toc37094604)

[Appendix E. Penetration Test Report 25](#_Toc37094605)

[Appendix F. Penetration Test and Scan Results Summary 26](#_Toc37094606)

List of Tables

[Table 1. Executive Summary of Risks 5](#_Toc37094561)

[Table 2. Personnel Interviews 8](#_Toc37094562)

[Table 3. Summary of Findings 12](#_Toc37094563)

[Table 4. Assessment Results 13](#_Toc37094564)

[Table 5. Summary of Assessment Results 14](#_Toc37094565)

[Table 6. Definition of Risk Levels 15](#_Toc37094566)

[Table 7. Detailed Findings 17](#_Toc37094567)

[Table 8. Summary of CIS Top 20 Controls 17](#_Toc37094568)

[Table 9. Summary of OWASP Top 10 17](#_Toc37094569)

[Table 10. Infrastructure Raw Scan Results 19](#_Toc37094570)

[Table 11. False Positive Reports by Infrastructure Scanner 19](#_Toc37094571)

[Table 12. Database Inventory Scan Results 21](#_Toc37094572)

[Table 13. Database Raw Scan Results 21](#_Toc37094573)

[Table 14. False Positives Generated by the Database Scanner 22](#_Toc37094574)

[Table 15. Inventory of Web Applications Scanned 23](#_Toc37094575)

[Table 16. Web Applications Raw Scan Results 23](#_Toc37094576)

[Table 17. False Positive Reports by Web Applications Scanner 24](#_Toc37094577)

[Table 18. IP Addresses and URLs for In-Scope Systems 25](#_Toc37094578)

[Table 19. Summary of Scan Results 26](#_Toc37094579)

[Table 20. Total Risk Findings 26](#_Toc37094580)

# Executive Summary

The primary purpose of this document is to provide a Security and Privacy Assessment Report (SAR) for [AE System] for the purpose of making risk-based decisions.

A Security and Privacy Assessment of [AE System] 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].

Table 1 below represents the aggregate risk identified from the assessment.

Table 1. Executive Summary of Risks

|  |  |
| --- | --- |
| **Risk Category** | **Number of Risks** |
| High | 0 |
| Moderate | 0 |
| Low | 0 |
| **Total Risks** | **0** |

# Introduction and Purpose

The Patient Protection and Affordable Care Act (ACA) program requires use of an independent third-party assessor to perform security and privacy assessment testing and to develop a SAR based on the outcomes of the assessment.

[Assesor Name] performed security and privacy testing for [Information System Acronym] in accordance with the [Information System Acronym] SAP, [SAP Date], [SAP Version #].

This SAR provides the [ AE] Information System Security Officer (ISSO), Senior Official for Privacy (SOP), and the Authorizing Officials (AOs) with the results of the assessment completed for the [Information System Acronym]. The SAR describes risks associated with the vulnerabilities identified during the [Information System Acronym] 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 AE and comprehensive Security and Privacy Assessment and Continuous Monitoring Plan developed using guidance from Minimum Acceptable Risk and Standards (MARS-E) [version #].

## Applicable Laws, Regulations, and Standards

By interconnecting with the CMS network and the CMS information system, the AE agrees to be bound by the AE Interconnection Security Agreement (ISA) and the use of the CMS network and information system in compliance with the ISA. The following applicable laws, regulations, and standards apply [the AE may also add other state laws, regulations, and standards as applicable]:

* Office of Management and Budget (OMB) Circular A-130, Appendix I: Responsibilities for Protecting and Managing Federal Information Resources
* Title 18 of the United States Code (U.S.C.) §641, Criminal Code: Public Money, Property, or Records
* Title 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information
* Health Insurance Portability and Accountability Act (HIPAA) of 1966 (Public Law [PL] 104-191)
* Patient Protection and Affordability Care Act (PPACA) of 2010
* Department of Health and Human Services (HHS) Regulation 45 Code of Federal Regulation (C.F.R.) §155.260 – Privacy and Security of Personally Identifiable Information
* HHS Regulation 45 C.F.R. §155.280 – Oversight and monitoring of privacy and security requirements
* The Privacy Act of 1974, Title 5 of the U.S.C. §552a. System of Records Notice citation: “Health Insurance Exchanges Program”, Title 78 of the Federal Register 8538, February 6, 2013
* The Patient Protection and Affordable Care Act of 2010 (PL 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (PL 111-152);
* Title 45 C.F.R. §155.260(b)
* Section 1943(b) of the Social Security Act (as added by section 2201 of the ACA)
* The Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite

## Scope

The assessor analyzed all assessment results to provide the [AE] ISSO, SOP, and the AOs 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 Acronym] System Security and Privacy Plan (SSP).

This document consists of a SAR for [Information System Name] [Information System Acronym] 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 Acronym] and is provided to support the [Name of AE] [Acronym of AE] program goals, efforts, and activities necessary to achieve compliance with the necessary security and privacy requirements.

The [AE] engaged [Assessor Name] to perform an onsite Security and Privacy Controls Assessment (SCA) of the [Information System Name] in order to determine:

* If the system is compliant with MARS-E [version #];
* 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:

[**Instructions:** 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. Include additional documents as necessary.

* Example: Operating system(s): Windows, Linux and version
* Example: Database and version #
* Example: Information System, and subcomponents
* Example: Web Applications and URLs

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

**Additional Instructions:** Security and privacy documentation will be reviewed for completeness and accuracy through this process, the assessor will gain insight to determine if all controls are implemented as described. The assessor’s review also augments technical control testing.

The assessor must review, at a minimum, the following required documents for assessment. Additional documents or supporting artifacts may be reviewed as necessary.

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

The following documents were assessed [This is a sample list, and it is not all inclusive]:

* 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.

The personnel selected to be interviewed had the following 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] |
| **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] |

# System Overview

## System Description

[**Instructions:** 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.]

## Purpose of System

[**Instructions:** 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.]

# Summary Report

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

## Summary of Findings

[**Instructions:** Provide a narrative summary of the findings relating to the security and privacy control families. Complete the Summary of Findings Table 3 for ALL findings from the assessment regardless of the type of test. Refer to subsection 5.1 for a description of the column headings.

The assessor must provide a total of number system risks that were identified for the information system. The assessor 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.

For example, many of the findings fall into the Access Control (AC) family due to the misconfiguration of the database and web application services, and overdue account reviews.

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

Most findings in this document 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 (each AE) uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Table 3. Summary of Findings

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

## Summary of Recommendations

For each finding, the assessor 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:

[**Instructions:** 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.]

# Detailed Findings Report

[**Instructions:** 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

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

The table below 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 [System Name] Security and Privacy Assessment Worksheet.

[**Instructions:** Add the numbers in the table

| Sample Table | | | | |
| --- | --- | --- | --- | --- |
| **Security Controls** | **Total** | **Met** | **Partially Met** | **Not Met** |
| AC – Access Control | 6 | 2 | 3 | 1 |
| AT – Awareness and Training | 4 | 2 | 1 | 1 |
| AU – Audit and Accountability | 7 | 3 | 2 | 2 |

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

Table 4. Assessment Results

| **Security Controls** | **Total** | **Met** | **Partially Met** | **Not Met** |
| --- | --- | --- | --- | --- |
| AC – Access Control | 0 | 0 | 0 | 0 |
| AT – Awareness and Training | 0 | 0 | 0 | 0 |
| AU – Audit and Accountability | 0 | 0 | 0 | 0 |
| CA – Security Assessment and Authorization | 0 | 0 | 0 | 0 |
| CM – Configuration Management | 0 | 0 | 0 | 0 |
| CP – Contingency Planning | 0 | 0 | 0 | 0 |
| IA – Identification and Authentication | 0 | 0 | 0 | 0 |
| IR – Incident Response | 0 | 0 | 0 | 0 |
| MA – Maintenance | 0 | 0 | 0 | 0 |
| MP – Media Protection | 0 | 0 | 0 | 0 |
| PE – Physical and Environmental Protection | 0 | 0 | 0 | 0 |
| PL – Planning | 0 | 0 | 0 | 0 |
| PM – Program Management | 0 | 0 | 0 | 0 |
| PS – Personnel Security | 0 | 0 | 0 | 0 |
| RA – Risk Assessment | 0 | 0 | 0 | 0 |
| SA – System and Services Acquisition | 0 | 0 | 0 | 0 |
| SC – System and Communications Protection | 0 | 0 | 0 | 0 |
| SI – System and Information Integrity | 0 | 0 | 0 | 0 |
| AP – Authority and Purpose | 0 | 0 | 0 | 0 |
| AR – Accountability, Audit, and Risk Management. | 0 | 0 | 0 | 0 |
| DI – Data Quality | 0 | 0 | 0 | 0 |
| DM – Data Minimization and Retention | 0 | 0 | 0 | 0 |
| IP – Individual Participation and Redress | 0 | 0 | 0 | 0 |
| SE – Security | 0 | 0 | 0 | 0 |
| TR – Transparency | 0 | 0 | 0 | 0 |
| UL – Use Limitation | 0 | 0 | 0 | 0 |
| **TOTAL CONTROLS** | **0** | **0** | **0** | **0** |

The number of controls that had one or more weaknesses identified during the assessment is listed below:

Table 5. Summary of Assessment Results

|  |  |
| --- | --- |
| **Control Assessment Category** | **Count** |
| Met | 0 |
| Partially Met | 0 |
| Not Met | 0 |
| **TOTAL** | **0** |

## Detailed Findings Table

[**Instructions:** This subsection provides a description of the columns in the Detailed Findings Table 7.

**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. Table 6 defines the risk levels.

Table 6. Definition of Risk Levels

| Rating | Definition of Risk Rating | |
| --- | --- | --- |
| High | Exploitation of the technical or procedural vulnerability will cause substantial harm to business processes. Significant political, financial, and legal damage is likely to result. |
| Moderate | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. |
| Low | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. |

**Control Number**

The Control Number column identifies the AE 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 20 Controls**

State whether the control falls under a CIS Top 20 controls area.

<https://www.cisecurity.org/controls/cis-controls-list/>

**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.

<https://owasp.org/www-project-top-ten/?gclid=EAIaIQobChMI5pfLhMKz5wIVGqSzCh0ragA3EAAYAyABEgKPoPD_BwE>

**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.

**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 assessor provides these suggestions to present guidance on a potential fix.

**POA&M Reference #**

Identify the corresponding POA&M reference number.

**Status**

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

Complete Table 7. Add rows as necessary.

After completing Table 7, complete Table 8, and Table 9 accordingly.

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

Table 7. Detailed Findings

| Row # | Weakness | Risk Level | Control # | CIS Top 20 Controls | OWASP Top 10 | Affected Systems | Finding | Failed Test Description | Actual Test Results | Corrective Actions | POA&M Reference# | Status |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

Table 8. Summary of CIS Top 20 Controls

|  |  |
| --- | --- |
| **Assessment Results** | **Count** |
| Met | 0 |
| Partially Met | 0 |
| Not Met | 0 |
| **TOTAL** | **0** |

Table 9. Summary of OWASP Top 10

|  |  |
| --- | --- |
| **Assessment Results** | **Count** |
| Met | 0 |
| Partially Met | 0 |
| Not Met | 0 |
| **TOTAL** | **0** |

1. Security and Privacy Assessment Worksheet

The completed Security and Privacy Assessment Worksheet has been submitted in a zip file along with this report.

[**Instructions:** Provide a copy of the completed Security and Privacy Assessment Worksheet for the security control assessments (Example of blank worksheet below).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CONTROLS DESCRIPTION | Examine | | Test | | Interview | | Comments |
| Artifacts | Result (Pass/Fail) | Methods and Objects | Result (Pass/Fail) | Personnel Interviewed | Result (Pass/Fail) |
| ACCESS CONTROL POLICY AND PROCEDURES |  |  |  |  |  |  |  |
| ACCOUNT MANAGEMENT |  |  |  |  |  |  |  |

**Examine:** Describe in detail how the control is implemented either through process, policy, or technical implementation.

**Test Methods and Objects:** This field further explains the asessment objective and also identifies specific action steps the assessment team has taken along with any additional evidence the team may have collected. If automated tools are utilized, describe the tool and how it satisfies the control requirement.

**Interview:** Identify for each control who or what role is responsible for its implementation.

**Result (Pass):** System provides control that mitigates vulnerability/threat.

**Result (Fail):** Control is not implemented. POA&Ms are needed to mitigate vulnerability/threat.

**Comments:** If the solution does not fully address each control requirement, document any compensating controls in place that reduce the residual risk.

**NOTE:** If a control is N/A, indicate why it is N/A.

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

1. 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 hosts and devices. The [Scanner Name, Vendor, and Version #] was used to scan the [Information System Acronym] infrastructure. [Number] % of the inventory was scanned. For the remaining inventory, the assessor 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 7).

* 1. Infrastructure Scans: Raw Scan Results

[**Instructions:** 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.

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

Table 10 indicates the files that are included.

Table 10. Infrastructure Raw Scan Results

| Title of the Document | Description | File Name  (Includes Extension) |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Infrastructure Scans: False Positive Reports

[**Instructions:** 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 11 indicates false positives that were generated by the infrastructure scanner.

Table 11. False Positive Reports by Infrastructure Scanner

| ID | Page and IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

1. Database Scan Results

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

* 1. Database Scans: Inventory of Databases Scanned

[**Instructions:** 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.

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

Table 12 presents the database inventory scan results.

Table 12. Database Inventory Scan Results

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

* 1. Database Scans: Raw Scan Results

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

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

Table 13 indicates the files that are included.

Table 13. Database Raw Scan Results

| Title of Document | Description | File Name  (Includes Extension) |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Database Scans: False Positive Reports

[**Instructions:** 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 indicates 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. Web Application Scan Results

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

[**Instructions:** 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.

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

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

Table 15 indicates 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* 1. Web Applications Scans: Raw Scan Results

[**Instructions:** 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.

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

Table 16 indicates the files that are included.

Table 16. Web Applications Raw Scan Results

| Title of Document | Description | File Name  (Includes Extension) |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Web Applications Scans: False Positive Reports

[**Instructions:** 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 17 Indicates false positives that was generated by the web applications scanner.

Table 17. False Positive Reports by Web Applications Scanner

| ID | IP Address | Scanner Severity Level | Finding | False Positive Explanation |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Penetration Test Report

[**Instructions:** The results reported in this appendix should be components identified in Section 3 of the Security and Privacy Controls Assessment Test Plan and should include the OWASP Top 10 results.

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

The scope of this assessment was limited to the [Information System Acronym] solution, including [List components here as documented in the Security and Privacy Test Plan Section 3 or] components. The assessor conducted testing of [Acronym of AE] activities from [Location] via an attributable internet connection.

Table 18 provides IP addresses and Uniform Resource Locators (URLs) for all the in-scope systems at the beginning of the assessment.

Table 18. IP Addresses and URLs for In-Scope Systems

| Application | IP/URL | OWASP Top 10 | Penetration Test Results |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Penetration Test and Scan Results Summary

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

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

Table 19 is a summary of all scan assessment results appropriately mapped to the risk level ratings.

Table 19. Summary of Scan Results

| Risk Level | OS Scans | Web Scans | DB Scans | Source Code | Penetration Test | Total |
| --- | --- | --- | --- | --- | --- | --- |
| High | 0 | 0 | 0 | 0 | 0 | 0 |
| Moderate | 0 | 0 | 0 | 0 | 0 | 0 |
| Low | 0 | 0 | 0 | 0 | 0 | 0 |
| **TOTAL** | **0** | **0** | **0** | **0** | **0** | **0** |

Table 20 summarizes the total risk findings scan testing.

Table 20. Total Risk Findings

| Risk Level | Risks from Scan Testing | Total Risks |
| --- | --- | --- |
| High | [#] | [#] ([#]% of Grand Total) |
| Moderate | [#] | [#]([#]% of Grand Total) |
| Low | [#] | [#]([#]% of Grand Total) |
| **TOTAL** | **[#]** | **[#]** |