Below are the descriptions for each of the columns in the "SAR-Detailed Findings" tab.

Row Number

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

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 table below defines the risk levels.

Rating	Definition of Risk Rating
Critical	Exploitation of the technical or procedural vulnerability will cause catastrophic harm to business processes. Catastrophic political, financial, and legal damage is likely to result.
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(ies) and control number(s) that is/are affected by the vulnerability. For example, "AC-1" or, if more than one control, "AC-3, CA-7".

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 'Failed Test Description' column 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' column provides 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.

POA&M Reference #

Identify the corresponding POA&M reference number, which is a unique number assigned to each POA&M entry that is used to track the weakness.

Recommendations

The 'Recommendations' column presents the recommended actions to resolve the vulnerability. The assessor provides these suggestions to present guidance on a potential fix.

Status

The 'Status' column provides status information, which includes when the vulnerability was identified, and any action(s) being taken to resolve it.

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

Findings relating to the security and privacy control families are listed in the "SAR-Detailed Findings" tab of the AE Security and Privacy Assessor Workbook.

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, PHI, FTI 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, PHI, and FTI by programs and information systems.
- **Data Quality and Integrity:** The organizations take reasonable steps to confirm the accuracy and relevance of PII, PHI, and FTI. 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/PHI/FTI 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, PHI, and FTI 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, PHI, and FTI.
- **Transparency:** Provides effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII, PHI,

and FTI generally and, where appropriate, to make an informed decision prior to providing PII, PHI, and FTI to an organization.

- **Use Limitation:** The organization (each AE) uses PII, PHI, and FTI internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

6.3 Scan Results

INFRASTRUCTURE

[**Instructions:** Indicate the infrastructure components that were scanned in the "SAR-Infrastructure Scan Results" tab of the AE Security and Privacy Assessor Workbook.

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

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. For the remaining inventory, the assessor performed a manual review of configuration files to analyze for existing vulnerabilities.

The [Scanner Name, Vendor, and Version #] was used to scan the [Information System Acronym] infrastructure. Findings as the result of the infrastructure scans are documented in the "SAR-Infrastructure Scan Results" tab of the AE Security and Privacy Assessor Workbook.

APPLICATIONS

[**Instructions:** Indicate the applications that were scanned in the "SAR-Application Scan Results" tab of the AE Security and Privacy Assessor Workbook.

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

The [Scanner Name, Vendor, & Version #] was used to scan the [Information System Abbreviation] applications. Findings as the result of the application scans are documented in the "SAR-Application Scan Results" tab of the AE Security and Privacy Assessor Workbook.

DATABASES

[**Instructions:** Indicate the databases that were scanned "SAR-Database Scan Results" tab of the AE Security and Privacy Assessor Workbook.

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

The [Scanner Name, Vendor, & Version #] was used to scan the [Information System Abbreviation] databases. Findings as the result of the database scans are documented in the "SAR-Database Scan Results" tab of the AE Security and Privacy Assessor Workbook.

SOURCE CODES

[**Instructions:** Indicate the web applications that were scanned "SAR-Source Code Scan Results" tab of the AE Security and Privacy Assessor Workbook.

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

The [Scanner Name, Vendor, & Version #] was used to scan the source codes on the [Information System Abbreviation] web applications. Findings as the result of the source code scans are documented in the "SAR-Source Code Scan Results" tab of the AE Security and Privacy Assessor Workbook.

PENETRATION TEST

[**Instructions:** The results reported in "SAR-Pen Test Results" tab of the AE Security and Privacy Assessor Workbook should be of the components identified in the SSP and the Penetration Test Plan.

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 SSP and the Penetration Test Plan]. The assessor conducted testing of [Acronym of AE] activities from [Location] via an attributable internet connection. The "SAR-Pen Test Results" tab of the AE Security and Privacy Assessor Workbook provides IP addresses and Uniform Resource Locators (URLs) for all the in-scope systems.

6.4 Raw Scan Results

[**Instructions:** Upload the raw scan results from all layers of the security system to the AE's folder on the State Exchange Resource Virtual Information System (SERVIS). Provide names of the files according to additional instructions in the "SAR-Raw Scan Files" tab of the AE Security and Privacy Assessor Workbook.

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

At the completion of the assessment, the [Acronym of AE] will upload the raw scan files to the AE's folder on the State Exchange Resource Virtual Information System (SERVIS). The names of the files containing the raw scan results from all layers of the [Information System Acronym] can be found in the "SAR-Raw Scan Files" tab of the AE Security and Privacy Assessor Workbook.

6.5 False Positive Results

[**Instructions:** Provide False Positive results for ALL layers of the security system by following the additional instructions in the "SAR-False Positives" tab of the AE Security and Privacy Assessor Workbook.

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

False Positive results for all layers of the [Information System Acronym] are documented in the "SAR-False Positives" tab of the AE Security and Privacy Assessor Workbook.

7. Summary of Recommendations

[**Instructions:** While all findings must be addressed, findings representing a critical or 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.]

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:

[Click here and type text.]

Appendix A. Acronym List

AC	Access Control, a Security Control family
ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
AP	Authority and Purpose, a Privacy Control family
AR	Accountability, Audit, and Risk Management, a Privacy Control family
AT	Awareness and Training, a Security Control family
BIOS	Basic Input Output System
CA	Security Assessment and Authorization, a Security Control family
CentOS	Community Enterprise Operating System
C.F.R.	Code of Federal Regulation
CIDR	Classless Inter-Domain Routing
CIS	Center for Internet Security
CM	Configuration Management, a Security Control family
CMP	Configuration Management Plan
CMS	Centers for Medicare & Medicaid Services
CP	Contingency Planning, a Security Control family
DISA	Defense Information Systems Agency
DNS	Domain Name System
DUA	Data Use Agreement
FISMA	Federal Information Security Management Act
FTI	Federal Tax Information
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HTTPS	Hypertext Transfer Protocol Secure
Hub	ACA Data Services Hub
IP	Internet Protocol
IR	Incident Response, a Privacy Control family
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISRA	Information Security Risk Assessment
ISSO	Information System Security Officer

MAC	Media Access Control
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MOU	Memoranda of Understanding
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OWASP	Open Web Application Security Project
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Planning, a Security Control family
PL	Public Law
POA&M	Plan of Action & Milestones
POC	Point of Contact
PPACA	Patient Protection and Affordability Care Act
RA	Risk Assessment, a Security Control family
ROE	Rules of Engagement
SAP	Security and Privacy Assessment Plan
SAR	Security and Privacy Assessment Report
SAT	Security Awareness Training
SCA	Security and Privacy Controls Assessment
SME	Subject Matter Expert
SOP	Senior Official for Privacy
SQL	Structured Query Language
SSP	System Security and Privacy Plan
STIG	Security Technical Implementation Guide
URL	Uniform Resource Locator
USGCB	United States Government Configuration Baseline
WORM	Write-Once-Read-Many
XSS	Cross-Site Scripting
XXE	XML External Entity