Centers for Medicare & Medicaid Services

Affordable Care Act (ACA) Health Insurance Administering Entity (AE)

Security and Privacy Assessment Plan (SAP) for the [Administering Entity (AE Acronym) System Name (System Acronym)] System

Prepared by: [Assessing Organization]

Version: [#.#]

Publication Date: [Publication Date]

Template v3.1, Dated April 25, 2022

<<Delete heading and table below before use>>

[Record of Template Changes]

Version Number	Version Date	Author/ Owner	A=Add M=Modify D=Delete	Description of Changes	Substantive Change [Y/N]
1.0	12/20/2019	LL	N/A	Document creation	N/A
1.1	4/6/2020	LL	M	Changed Assessment worksheet name. Updated Appendix A. Minor language/grammar corrections and formatting changes.	N
2.0	1/20/2021	Chris Day	A, M, D	Restructure document layout. Removed tables that were added to associated Assessor Workbook. Updated instructions. Consolidated Application sections. Removed appendices. Language/grammar corrections and formatting changes.	Y
2.1	9/24/2021	Luis Effio, Danielle Andrews	A, M, D	Added SAW instructions to various sections in the document. Updated formatting and language.	Y
3.0	1/28/2022	Luis Effio, Danielle Andrews	A, M, D	Re-added tables previously moved to the SAW and updated instruction language in Section 2. Adjusted language in Sections 2.7, 2.8 and 3.1. Updated table names in Section 4. Updated the Finalization/Completion activity in Table 14. Updated Acronyms throughout document and the Acronym List. Made Record of Template Changes Table removeable. Formatting changes.	Y
3.1	4/25/2022	Luis Effio, Danielle Andrews	A	Added Table 11 to Section 5.2. Added discloser content control box to Section 7.1.	N

<<General Instructions for Completing this Plan:

IMPORTANT: This page contains instructions that should be deleted prior to distribution of the completed draft or final Security and Privacy Assessment Plan (SAP).

Delete all blue instructional text and unused content control boxes and ensure that the font color has been normalized with the surrounding text prior to final submission.

The blank template is not subject to limitations on use or disclosure; however, the completed template will contain sensitive proprietary information and may only be disclosed as described under the terms of this SAP.

Instructions for Administering Entities (AEs) are provided within the double arrows << … >>. Ensure to provide the required information within the brackets […], delete any remaining instructions, and normalize the font with the surrounding text.

NOTE: This SAP must be submitted to Centers for Medicare and Medicaid Services (CMS) for review prior to the assessment. After this SAP has been completed, the assessor must meet again with the AE to present the draft SAP and make necessary changes prior to finalization.

General Instructions for the Kickoff Meeting:

The SAP must be jointly completed and agreed to before the start of the assessment by both the AE and the assessor. To expedite the process, this may be done during an assessment kickoff meeting.

The goal of the kickoff meeting is to obtain the necessary assessment scope information outside of that which was in the contract statement of work. The assessor must obtain this information to accurately complete the SAP.

The AE should be prepared to bring the necessary resources to the kickoff meeting or ensure the availability of resources to expedite the process during the meeting.>>

Security and Privacy Assessment Plan

Prepared by:

Organization Name: [Assessing Organization]

Street Address: [Street Address]

Suite/Room/Building: [Suite/Room/Building]

City, State Zip: [City, State, Zip]

Prepared for:

Organization Name: [Administering Entity]

Street Address: [Street Address]

Suite/Room/Building: [Suite/Room/Building]

City, State Zip: [City, State, Zip]

Revision History

Date	Description	Version of SAP	Author
[Choose]	[Insert Revision Description]	[#.#]	[Author]

<<Add more rows as needed.>>

Table of Contents

List of Tables

1 Introduction

[AE Name or AE Acronym] [System Name or System Acronym] will be assessed by [Assessing Organization], the assessor, and should have a complete and implemented System Security and Privacy Plan (SSP) prior to starting the security and privacy assessment.

The use of an independent assessment team reduces the potential for conflicts of interest that can occur in verifying the implementation status and effectiveness of the security and privacy controls. Centers for Medicare & Medicaid Services (CMS) provides guidance for employing independent assessors in the *Framework for Independent Assessment of Security and Privacy Controls*[1]:

> *An assessor is independent if there is no perceived or actual conflict of interest with respect to the developmental, operational, and/or management chain associated with the information system and the determination of security and privacy control effectiveness. The Administering Entities (AE's) designated security and privacy official(s) must ensure that there is a complete separation of duties between the staff associated with the information system and the assessor or assessment team conducting the Security Control Assessment (SCA).*

The assessor's role is to provide an independent security and privacy assessment of the [System Name or System Acronym] system and to maintain the integrity of the audit process. The assessor must attest to their independence and objectivity in completing the assessment and that neither the AE nor the assessor took any actions that might impair the objectivity of the assessment findings in Section 7.6.

1.1 Applicable Laws, Regulations, and Standards

An Interconnection Security Agreement (ISA) with Centers for Medicare & Medicaid Services (CMS) is required if a system-to-system connection is made to the Federal Data Services Hub (Hub) to exchange data with CMS.

The Patient Protection and Affordable Care Act (ACA) AE Systems should also maintain ISAs and Memoranda of Understanding (MOU) between all additional Information Technology (IT) systems that connect to and share data or resources with the AE System. Laws, regulations, and standards that apply include the following:

- Federal Information Security Modernization Act of 2014 (FISMA), December 2014.
- Office of Management and Budget (OMB) Circular A-130, Appendix I: *Responsibilities for Protecting and Managing Federal Information Resources*, July 2016.
- Title 18 of the United States Code (U.S.C.) §641, *Criminal Code: Public Money, Property, or Records*, January 2012.
- Title 18 of the United States Code (U.S.C.) § 1905, *Criminal Code: Disclosure of Confidential Information*, January 2011.

[1] Available at https://zone.cms.gov/document/framework-independent-assessment-security-and-privacy-controls

- Health Insurance Portability and Accountability Act (HIPAA) of 1966 (Public Law [PL] 104-191), August 1996.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk*, March 2011.
- The Patient Protection and Affordable Care Act of 2010 (ACA) (PL 111-148), March 2010.
- The Patient Protection and Affordable Care Act of 2010 (ACA) (PL 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (PL 111-152), March 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 (PII)*, October 2014.
- Department of Health and Human Services (HHS) Regulation 45 Code of Federal Regulation (C.F.R.) §155.280, *Oversight and Monitoring of Privacy and Security Requirements*, October 2015.
- The Privacy Act of 1974, Title 5 of the Code of Federal Regulation (U.S.C.) §552a. System of Records Notice citation: "Health Insurance Exchanges Program", Title 78 of the Federal Register 8538, February 2013.
- Department of Health and Human Services (HHS) Title 45 C.F.R. §155.260(b) – *Privacy and Security of Personally Identifiable Information (PII) for Exchange Functions*, October 2014.
- Social Security Act, Section 1943(b) (as added by Section 2201 of the Patient Protection and Affordable Care Act of 2010 (ACA) (PL 111-148), March 2010.
- The Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite.

<<List additional state laws, regulations, and standards, as necessary.>>

1.2 Purpose

This SAP documents all testing planned in order to validate the security and privacy controls for the [System Name or System Acronym] system. The plan also identifies all system components being tested. The information included within this SAP will assist in the preparation of the Security and Privacy Assessment Report (SAR). This SAP has been completed by [Assessing Organization] for the benefit of [AE Name or AE Acronym]. The *Framework for Independent Assessment of Security and Privacy Controls* requires:

- System compliance with MARS-E
- Underlying infrastructure security posture
- System and data security and privacy posture
- Proper security configuration associated with the database or file structure storing the data
- Technical, managerial, and organizational adherence to the organization's security and privacy program, policies, and guidance

2 Scope

2.1 System or Application Details

<<Complete Table 1 with the name of the system(s) and/or application(s) that are scheduled for testing. Briefly describe the system components. The description can be copied from the description in the SSP.

Complete Table 2 with the geographic location of all the components that will be tested.>>

Table 1 provides the information system(s) and/or application(s) scheduled for testing.

Table 1. Information System Name and Description

Information System Name	Information System Description
[Insert System Name]	[Insert System Description]

<<Add more rows as needed.>>

Table 2 provides the physical locations of all components to be assessed.

Table 2. Information System Components

Login URL* Data Center Site Name	Physical Address	Description of Components
[Insert Login URL]	[Insert Physical Address]	[Insert Description]

<<Add more rows as needed.>>

** Uniform Resource Locator (URL)*

2.2 Roles Slated for Testing

<<Roles to be tested should correspond to those roles listed in the SSP. Role testing will be performed to challenge the authorization restrictions for each role. The assessor will access the system while logged in as different user types and attempt to perform restricted functions as unprivileged users.>>

Table 3 below indicates the roles that are slated for testing.

Table 3. Roles Slated for Testing

User Role Name	Test User ID*	User Role Functions
[Insert User Role Name]	[Insert Test User ID]	[Insert User Role Responsibilities]

<<Add more rows as needed.>>

** Identification (ID)*

2.3 IP Addresses Slated for Testing

<<List the IP address of all systems that will be tested. Obtain this information from the SSP and the organization.

NOTE: IP addresses found in the SSP must be consistent with the boundary. All scans must be fully authenticated. In addition, unique identifiers (e.g., Media Access Control (MAC) address or hostname), may be used instead of the IP address. Organizations must ensure that the inventory is current before testing, and that the inventory and components to be tested are in agreement.>>

IP addresses and network ranges of the system that will be tested are noted in Table 4.

Table 4. IP Addresses Slated for Testing

IP Address(s) or Ranges	Hostname	Software & Version	Function
[Insert IP Address(s) or Ranges]	[Insert Hostname]	[Insert Software & Version]	[Insert Function]

<<Add more rows as needed.>>

2.4 Infrastructure Slated for Testing

<<Identify all infrastructure components that will be in scope for this assessment using the table below. You will need to obtain this information from the SSP and the organization.

NOTE: Infrastructure components found in the SSP must be consistent with the boundary. If additional infrastructure components are discovered that were not included in the SSP, note the finding(s), and advise the organization to update the inventory and boundary information in the SSP. The assessor must ensure that the inventory and components are current and validated before testing.>>

Table 5 below indicates the infrastructure and/or network components as well as major applications slated for testing.

Table 5. Infrastructure and Network Components Slated for Testing

Product Model & Vendor Names	Model Version Number	Operating System	Function / Description	Physical / Virtual Component
[Insert Product Model and Vendor Names]	[Insert Model Version Number]	[Insert Operating System]	[Insert Function / Description]	[Insert Physical / Virtual Component]

<<Add more rows as needed.>>

2.5 Web Applications Slated for Testing

<<Insert any URLs and the associated login IDs that will be used for testing. Only list the login URL. Do not list every URL that is inside the login in the below table. In the Function column, indicate the purpose that the web-facing application plays for the system (e.g., control panel to

build virtual machines). In addition, Organizations may use any unique identifier (e.g., MAC address or hostname), instead of the IP address.

NOTE: The Assessor must test for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Application Security Risks[2].>>

Activities employed to perform role testing on web applications may include capturing POST and GET requests for each function. The various web-based applications that make up the system, the logins, and their associated roles that will be used for testing are noted by URL in Table 6 below.

Table 6. Web Applications Slated for Testing

Login URL	Login ID	IP Address of Login Host	Function
[Insert Login URL]	[Insert Login ID]	[Insert IP Address of Login Host]	[Insert Function]

<<Add more rows as needed.>>

2.6 Databases Slated for Testing

<<Insert the hostnames, IP address, and any relevant additional information on the databases that will be tested. All scans must be fully authenticated. In addition, organizations may use any unique identifier (e.g., MAC address or hostname), instead of the IP address.>>

Table 7 below indicates the system database(s) slated for testing.

Table 7. Databases Slated for Testing

Database Name	Hostname	IP Address	Additional Info
[Insert Database Name]	[Insert Hostname]	[Insert IP Address]	[Insert Additional Info]

<<Add more rows as needed.>>

2.7 Documents to be Assessed

<<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 the following required documents at a minimum for the assessment. Additional documents or supporting artifacts may be reviewed, as necessary.>>

At a minimum, the following documents will be assessed:

- Business Agreement with Data Use Agreement (DUA)
- Configuration Management Plan (CMP)

[2] Available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- Contingency Plan and Test Results
- Plan of Action and Milestones (POA&M)
- Final SSP
- 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 and agreements to collect, use, and disclose PII and Privacy Act Statements
- Security Awareness Training (SAT) Plan and Training Records
- ISAs
- Information Security Risk Assessment (ISRA)
- Governance documents and privacy policy documentation describing the AE privacy risk assessment process, documentation of privacy risk assessments performed by the organization

<<List additional documents to be reviewed, as necessary.>>

2.8 Security and Privacy Controls to be Assessed

<<During the assessment, the assessor must evaluate the security and privacy controls to determine whether they are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the information system, according to MARS-E requirements. The assessor's evaluation will complement the document review.>>

The assessor will complete a [Choose an item.] assessment to of the security and privacy controls, using MARS-E version [#.#]. All [System Name or System Acronym] security and privacy controls can be found in the MARS-E SSP. The assessment will apply to [Choose Year] controls [as well as any applicable supplemental controls], which are identified in the Security and Privacy Assessor Workbook (SAW)[3].

2.9 Assumptions/Limitations

<<The assessor must edit the assumptions and limitations below as necessary for each unique engagement. The assessor may add more assumptions and/or limitations, as necessary.>>

1. [The AEs resources, including documentation and individuals with knowledge of the AEs systems, applications, and infrastructure and associated contact information, will be available to the Assessing Organizations assessment staff during the scheduled assessment timeframe and testing activities in order to complete the assessment.
2. The AE will provide login account information/credentials necessary to perform authenticated scans of devices and applications.

[3] Available at https://zone.cms.gov/document/ae-security-and-privacy-assessor-workbook

3. The AE will permit the Assessing Organizations assessment staff to connect testing laptops to the AEs networks defined within the scope of this assessment.
4. The AE will permit communication from the assessor testing appliances to an internet-hosted vulnerability management service to permit the analysis of vulnerability data.
5. Security and privacy controls that have been identified as "Not Applicable" in the SSP must be accompanied with an explanation and will be verified as such; further testing will not be performed on these controls.
6. Significant upgrades or changes to the infrastructure and components of the system undergoing testing will not be performed during the security and privacy assessment period.
7. For onsite control assessment, AE personnel will be available should the Assessing Organization's assessment staff determine that either after-hours work or weekend work is necessary to support the security and privacy assessment.]

3 Scanning Tools and Procedures

All scans performed must be authorized by the [Assessing Organization] Team and the AE Representative prior to conducting the assessment. This SAP will authorize the [Assessing Organization] Team to use the tools indicated in Table 8 to perform scans on the [System Name or System Acronym] system. The AE will also have the option to perform scans on their own system(s) with the guidance and supervision of the [Assessing Organization] Team. Authorization signatures from [Assessing Organization] and the AE Representative are located in Section 7.6.

Table 8. Scanning Tools and/or Procedures

Test to be Performed/Purpose	Tool or Procedure	What will be Tested
[Ex. Operating System Scan]	[Ex. Nessus]	[Ex. Internal boundary complete network]
[Ex. Web Applicable scan]	[Ex. HP WebInspect]	[Ex. Websites]
[Ex. Web Applicable scan]	[Ex. Burp Suite]	[Ex. Applications]
[Ex. Open Ports scan]	[Ex. Zenmap, Nmap]	[Ex. Any open ports]
[Ex. Database scan]	[Ex. DbProtect]	[Ex. Database configuration]

<<Add more rows as needed.>>

4 Test Roles

4.1 Security and Privacy Assessment Team

<<List the members of the independent assessment team and the role each member will play in the following table. Include team members' contact information.

Security and privacy control assessors play a unique role in testing system or application security and privacy controls. NIST SP 800-39, *Managing Information Security Risk* states:

> *The assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).>>*

The Assessment Team consists of individual(s) from [Assessing Organization], which are located at the following address: [Assessor Address]. Information about [Assessing Organization] can be found at the following URL: [Assessor URL].

Table 9 below identifies the members of the Assessment Team.

Table 9. [Assessing Organization] Assessment Team

Name	Role	Email Address
[Insert Name]	[Insert Role]	[Insert Email Address]

<<Add more rows as needed.>>

4.2 [AE Name or AE Acronym] Points of Contact

<<The assessor must obtain at least two Points of Contact (POCs) from the AE to use for testing communications.>>

Table 10 below identifies [AE Name or AE Acronym] Points of Contact (POCs) that the testing team can contact should they need guidance or clarification.

Table 10. [AE Name or AE Acronym] POCs

Name	Role	Email Address
[Insert Name]	[Insert Role]	[Insert Email Address]
[Insert Name]	[Insert Role]	[Insert Email Address]

<<Add more rows as needed.>>

5 Security and Privacy Controls Assessment Methodology

5.1 Overview

The assessor will perform an assessment of the security and privacy controls using the methodology described in the MARS-E Document Suite[4]. The results of testing the security requirements will be summarized in the SAR along with the information that notes whether the

[4] Available at https://zone.cms.gov/document/minimum-acceptable-risk-standards-exchanges-mars-e-suite

control is satisfied or not.

The SCA methodology (described in this document) originates from the standard CMS methodology used in the assessment of all CMS internal and business partner information systems.

Assessment procedures for testing each security and privacy control are located in the MARS-E SSP. A detailed assessment plan should be prepared using these security and privacy control assessment procedures. If necessary, modify or supplement the procedures to evaluate the system's vulnerability to different types of threats, including those from the insider, the Internet, or the network. The assessment methods include examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls.

This assessment provides the independent assessor with an accurate understanding of the security and privacy controls in place by identifying the following:

- Application or system vulnerabilities, the associated business and system risks, and potential impact
- Weaknesses in the configuration management process such as weak system configuration settings that may compromise the Confidentiality, Integrity, and Availability (CIA) of the system
- AE policies not followed
- Major documentation omissions and/or discrepancies

5.2 Tests and Analysis Performed

The SCA includes tests that analyze the application or system and the associated infrastructure. The tests begin with high-level analysis of the application or system and increase in specificity to eventually include an analysis of each supporting component. Tests and analysis performed during an assessment should include the following:

- Security and privacy controls technical testing
- Adherence to the organization's security and privacy program, policies, and guidance
- Network and component scanning
- Configuration assessment
- Documentation review
- Personnel interviews
- Observations

Table 11 identifies the application(s) or system(s) and the associated infrastructure.

<<Insert all hardware and/or software that will be tested during this assessment.>>

Table 11. System/Application Configuration

Hardware/Software Name	Hardware/Software Version	Benchmark	Benchmark Version
[Insert Hardware or Software Name]	[Insert Hardware or Software Version]	[Insert Benchmark]	[Insert Benchmark Version]

<<Add more rows as needed.>>

5.3 Security and Privacy Controls Technical Testing

Typically, the assessment staff provides user access to the system to conduct the application or system security technical testing. To perform a thorough assessment of the application or system, application-specific user accounts that reflect the different user types and roles are created for the technical assessor. By providing the technical assessor with these accounts, the assessor can test applications and system security and privacy controls that might otherwise not be tested. The assessors should not be given a user account with a role that would allow access to Protected Health Information (PHI) or Federal Tax Information (FTI) in any application or database.

The technical assessor attempts to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities such as buffer overflows and password compromises. The assessor must use caution to ensure no inadvertent altering of important system settings that may disable or degrade essential security or business functions. Since many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify proposed tools that pose a risk to the computing environment in the assessment plan. Furthermore, any testing that could potentially expose PII, PHI, or FTI must be performed under the direct supervision of an authorized individual who is responsible for the data and can monitor the assessor's actions and take appropriate action to protect any data that is exposed.

The lists below include common test procedures and techniques of the technical assessment.

Test Procedures:

- Examination of the implemented access controls and identification and authorization techniques (e.g., log-on with easily guessed/default passwords)
- Test to determine if the system is susceptible to cross-site scripting (XSS), Structured Query Language (SQL) injection, and/or other commonly exploited vulnerabilities
- Attempt to alter database management system settings
- Attempt to access hidden URLs
- Review of application-specific audit log configuration settings
- Determination if sensitive information is encrypted before being passed between the system and browser

Test Techniques:

- Broken Authentication and Session Management
- Sensitive Data Exposure

- XML External Entity (XXE)
- Broken Access Control
- Security Misconfiguration
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

5.4 Network and Component Scanning

In order to gain an understanding of the network and component infrastructure security posture, the SCA includes network-based scans of all in-scope network components to determine ports, protocols, and services running on each component. This provides a basis for determining the extent to which the system control implementation meets security and privacy control requirements. The results of these scans are used in conjunction with the configuration assessment.

5.5 Configuration Assessment

The purpose of the configuration assessment is to determine if AE security requirements are implemented correctly in the application, system, or system environmental components within the boundary of the application. The process for performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the AE security and privacy requirements
- Review access to system and databases for default user accounts
- Test firewalls, routers, systems, and databases for default configurations and user accounts
- Review firewall access control rules against the AE security requirements
- Determine consistency of system configuration with the AE-documented configuration

5.6 Documentation Review

The assessor must review all security and privacy documentation for completeness and accuracy. Through this process, the assessor will gain insight to determine if all controls are implemented as described. The review also augments technical control testing. For example, if the MARS-E control stipulates that the password length for the information system is required to be eight characters, the assessor must review the AE password policy or the SSP to make sure the documented password length is eight characters. During the technical configuration assessment, the assessor must confirm that passwords are actually configured in accordance with applicable AE documentation.

Table 12 below provides a list of the core security documents to be reviewed by the assessor.

Table 12. Core Security and Privacy Documentation

Document Name	MARS-E Control Family	MARS-E Control Number
System Security Plan (SSP)	Planning (PL)	PL-2: Security System Plan
Configuration Management Plan (CMP)	Configuration Management (CM)	CM-9: Configuration Management Plan
Contingency Plan	Contingency Planning (CP)	CP-2: Contingency Plan
Contingency Plan Test Plan and Results	Contingency Planning (CP)	CP-4: Contingency Plan Testing
Incident Response Plan (IRP)	Incident Response (IR)	IR-8: Incident Response Plan
Incident Response Plan (IRP) Test Plan	Incident Response (IR)	IR-3: Incident Response Testing and Exercises
Security Awareness Training (SAT) Plan	Awareness and Training (AT)	AT-3: Role-Based Security Training
Training Records	Awareness and Training (AT)	AT-4: Security Training Records
Interconnection Security Agreements (ISA)	Security and Assessment Authorization (CA)	CA-3: System Interconnections
Plan of Action and Milestones (POA&M)	Security and Assessment Authorization (CA)	CA-5: Plan of Action and Milestones
Information Security Risk Assessment (ISRA)	Risk Assessment (RA)	RA-3: Risk Assessment
Privacy Impact Assessment (PIA) or other privacy documents	Authority and Purpose (AP)	AP-1: Authority to Collect
Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PII and Privacy Act Statements	Authority and Purpose (AP)	AP-2: Purpose Specification
Governance documents and privacy policy	Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program
Documentation describing the AE privacy risk assessment process, documentation of privacy risk assessments performed by the organization	Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment

5.7 Personnel Interviews

The assessor will conduct personnel interviews to validate that security and privacy controls are implemented, staff understand and follow documented control implementations, and updated documentation is appropriately distributed to staff. The assessor will interview business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. Interviews will be 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 SCA test plan will identify the designated Subject Matter Experts (SMEs) interviewed. These SMEs should have specific knowledge of overall security and privacy requirements as well as a detailed understanding of the system's operational functions.

Table 13 below provides the personnel selected to be interviewed.

Table 13. Personnel Interviews

Title	Name of Person	Scheduled Interview Date	Comments
Business Owner(s)	[Insert name]	[Choose date]	[Insert comments]
Application Developer	[Insert name]	[Choose date]	[Insert comments]
Configuration Manager	[Insert name]	[Choose date]	[Insert comments]
Contingency Planning Manager	[Insert name]	[Choose date]	[Insert comments]
Database Administrator	[Insert name]	[Choose date]	[Insert comments]
Data Center Manager	[Insert name]	[Choose date]	[Insert comments]
Facilities Manager	[Insert name]	[Choose date]	[Insert comments]
Firewall Administrator	[Insert name]	[Choose date]	[Insert comments]
Human Resources Manager	[Insert name]	[Choose date]	[Insert comments]
Information System Security Officer	[Insert name]	[Choose date]	[Insert comments]
Privacy Program Manager	[Insert name]	[Choose date]	[Insert comments]
Privacy Officer	[Insert name]	[Choose date]	[Insert comments]
Media Custodian	[Insert name]	[Choose date]	[Insert comments]
Network Administrator	[Insert name]	[Choose date]	[Insert comments]
System Administrators	[Insert name]	[Choose date]	[Insert comments]
System Owner	[Insert name]	[Choose date]	[Insert comments]
Program Manager	[Insert name]	[Choose date]	[Insert comments]
Training Manager	[Insert name]	[Choose date]	[Insert comments]

Although the initial identification of interviewees is determined when the assessment plan is prepared, additional staff may be identified as the interview process proceeds.

5.8 Observations

The assessor also observes personnel behavior and the in–place, physical environmental controls, as applicable, to determine if staff follow the security and privacy policies, procedures and controls related to the physical environment. For example, the assessor is required to observe:

- Processes associated with issuing visitor badges
- Requests for identification prior to visitor badge issuance
- Handling of output materials, including the labeling and discarding of output
- Equipment placement to prevent "shoulder surfing" or viewing from windows and open spaces
- Physical security associated with media protection, such as locking of telecommunication and wiring closets and access to facilities housing the system

6 Assessment Schedule

<<Table 14 is a sample and provides suggested tasks and milestones in the assessment process. Assessment tasks may vary between assessments. Remove/add tasks as necessary and populate Start/Finish dates or insert an existing schedule.

This schedule must be presented to the AE by the assessor at the kickoff meeting. The Information System Security Officer (ISSO) and Senior Official for Privacy (SOP) must be invited to the meeting that presents the schedule to the AE. After the assessor presents the testing schedule to the AE at the kickoff meeting, the assessor must first make any necessary updates to the schedule and this document. The assessor must then send an updated version to the AE, with copies to the ISSO and the SOP.>>

Table 14 below provides the assessment schedule. All parties must agree on the tasks and durations.

Table 14. Schedule of Activities

Task Name	Start Date	Finish Date
Hold Kickoff Meeting	[Choose Date]	[Choose Date]
Develop Draft SAP	[Choose Date]	[Choose Date]
Hold Meeting to Review/Concur upon SAP	[Choose Date]	[Choose Date]
Finalize SAP	[Choose Date]	[Choose Date]
Review the [System Name or System Acronym] system Documentation	[Choose Date]	[Choose Date]
Conduct Interviews of [AE Name or AE Acronym] Staff	[Choose Date]	[Choose Date]
Perform Evaluation/Testing	[Choose Date]	[Choose Date]
Develop Draft SAR	[Choose Date]	[Choose Date]
Draft SAR Delivered to AE	[Choose Date]	[Choose Date]
Hold Issue Resolution Meeting	[Choose Date]	[Choose Date]
Finalize SAR	[Choose Date]	[Choose Date]
Send Final Version of SAR to [AE Name or AE Acronym]	[Choose Date]	[Choose Date]

Your active participation is crucial to the successful and timely completion of this assessment. Any shortcomings (such as not obtaining SAP signatures on time, not providing proper access or accounts on time, not being available for interviews, not returning evidence by due dates, etc.) will cause the assessment to be rescheduled based on the next availability on the assessment calendar, or continuation of the assessment with findings for missing items. Review the schedule above to ensure availability and communicate any obstacles you foresee.

Table 15 below provides the activities and responsibilities for this assessment.

Table 15. Activities and Responsibilities

Activities	Assessor Responsibilities	AE Personnel Responsibilities
Planning	• Review SSP and other documents provided • Deliver SAP • Conduct kickoff meeting • Provide a project schedule • Send invitations for agreed interview and demo times	• Attend kickoff • Review draft documents • Review schedule and notify assessment team immediately of any issues/conflicts • Ensure dates are provided for interview availability • Return SAP with completed inventory and targets URLs
Interviews/Test Prep Goals: • All interviews, demos are conducted • Artifact lists provided • Connectivity to assets and accounts are confirmed	• Conduct all interviews and demonstrations • Provide artifact request list after each interview and within one (1) business day of the last interview • Finalize SAP and obtain signatures • Test access to targets from source IP • Test accounts to ensure authentication and proper account privileges • Work with AE administrator to meet goals	• Ensure proper individuals are available for interview • Begin to provide evidence from interviews • Full review and signed SAP • Ensure access to all targets from source IP • Create and provide all test accounts • Work with testers to troubleshoot connectivity and access
Evidence Review/Testing	• Analysts analyze evidence • Tester runs all automated scans and any verification testing	• All evidence is returned by date provided • AE tester POC is available for any issues (account reset, connectivity loss, etc.). Response time should be within two (2) hours. • AE personnel are available for any follow up questions
Reporting	• Assessment team is working on the draft SAR and associated draft Security and SAW • Issue draft SAR and associated draft SAW by the end of the week	• AE personnel are available for any follow up questions
Finalization/Completion	• Answer any questions on the draft SAR/SAW	• Review draft SAR/SAW and provide any comments or

Activities	Assessor Responsibilities	AE Personnel Responsibilities
	• Schedule and attend debrief if requested • Update final SAR/SAW if necessary • Ensure final SAR and SAW are issued within five (5) business days of debriefing	schedule debrief within five (5) business days • Obtain system owner signature on final SAR and SAW within two (2) days of final issuance

7 Rules of Engagement

<<The assessor must edit the Rules of Engagement (ROE) as necessary. Both the assessor and AE must sign the final version of the ROE.>>

The Rules of Engagement (ROE) describes proper notifications and disclosures between the owner of the systems or applications being tested and the assessor. The ROE includes information about automated scan targets and IP address origination information of the automated scans (and other testing tools). The information provided in the preceding sections of this document, along with the agreed-upon and signed ROE, will serve as the ROE.

7.1 Disclosures

<<Add disclosures, as necessary. If testing will be conducted from an internal location, identify at least one network port with access to all subnets/segments to be tested. By identifying the IP addresses from where the security testing will be performed, the AE will understand that the rapid and high-volume network traffic is not an attack and is part of the testing performed by the assessor.>>

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. [Enter any additional disclosures.]

All scans will originate from the following IP address(es):

- [List IP addresses]

7.2 Test Inclusions

<<The inclusions listed are default test inclusions. The assessor must edit these inclusions as necessary for each unique engagement. The assessor may add more test inclusions, as necessary.>>

Security testing may include the following activities:

- [Port scans and other network service interaction and queries
- Network sniffing, traffic monitoring, traffic analysis, and host discovery
- Attempted logins or other use of systems, with any account name/password
- Attempted SQL injection and other forms of input parameter testing
- Use of exploit code for leveraging discovered vulnerabilities

- Password cracking via capture and scanning of authentication databases
- Spoofing or deceiving servers regarding network traffic
- Altering running system configuration except where denial of service would result
- Adding user accounts]

7.3 Test Exclusions

<<The exclusions listed are default test exclusions. The assessor must edit these exclusions as necessary for each unique engagement. The assessor may add more test exclusions, as necessary.>>

Security testing will not include any of the following activities:

- [Changes to assigned user passwords
- Modification of user files or system files
- Intentional viewing of the AEs staff email, Internet caches, and/or personnel cookie file]

7.4 End of Testing

[Assessing Organization] will notify the designated [AE Name or AE Acronym] senior security POC when security testing has been completed.

7.5 Communication of Test Results

Email and reports on all security testing will be encrypted according to [AE Name or AE Acronym] requirements. Security testing results will be sent and disclosed to the individuals at [AE Name or AE Acronym] within [#] days after security test has been completed.

The results of testing the security requirements will be summarized in the SAR and associated SAW.

The SAR and associated SAW will be reviewed to verify that each of the CMS requirements noted in the checklist is included in the report and analyzed to determine if the information provided adequately addresses the requirement.

The assessor will indicate whether each requirement is:

- **Met:** The requirement has been completely satisfied and no additional information needs to be documented.
- **Partially Met:** The requirement has been partially satisfied but there is still missing information as explained in the Comments column.
- **Not Met:** The requirement has not been satisfied and any additional information noting the reasons are provided in the Comments column.
- **N/A:** The requirement is not applicable to the system or security and privacy assessment that is being evaluated and the reason that it is not applicable is explained in the Comments column.

7.6 Signatures

The following individuals at [Assessing Organization] and [AE Name or AE Acronym] have been identified as having the authority to agree to security testing of the [System Name or System Acronym] system. The assessor attests to their independence and objectivity throughout the security and privacy assessment.

The following individuals acknowledge the foregoing SAP and ROE and agree to the tests and terms set forth in the plan.

[Assessing Organization] Representative	**[AE Name or AE Acronym] Representative**
(Name)	(Name)
(Signature) (Date)	(Signature) (Date)

Appendix A. Penetration Testing

<<The Assessor must attach a file containing the Penetration Test Plan or include the plan in this Appendix.

Penetration testing must include, in part, the security testing scenarios found in Section 5.3.

The AE will understand that the rapid and high-volume network traffic is not an attack and is part of the testing.>>

A penetration test will be performed to validate the vulnerabilities identified during the scanning phase, and to investigate other attack vectors through reconnaissance.

See [Choose an item.] for the Penetration Test Plan for this assessment.

[Penetration Test Plan details. This content control box can be deleted if the plan is attached.]

Appendix B. Acronym List

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
C.F.R.	Code of Federal Regulation
CA	Security Assessment and Authorization, a Security Control family
CIA	Confidentiality, Integrity, and Availability
CIDR	Classless Inter-Domain Routing
CM	Configuration Management, a Security Control family
CMP	Configuration Management Plan
CMS	Centers for Medicare & Medicaid Services
CP	Contingency Planning, a Security Control family
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
Hub	Federal Data Services Hub
ID	Identification
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
IT	Information Technology
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

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
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
SAW	Security and Privacy Assessor Workbook
SCA	Security and Privacy Controls Assessment
SME	Subject Matter Expert
SOP	Senior Official for Privacy
SP	Special Publication
SQL	Structured Query Language
SSP	System Security and Privacy Plan
U.S.C	United States Code
URL	Uniform Resource Locator
XSS	Cross-Site Scripting
XXE	XML External Entity