Centers for Medicare & Medicaid Services

Affordable Care Act (ACA) Health Insurance Administering Entity

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

Prepared by [Assessor Name]

Version [#]

Publication Date: [MM DD, YYYY]

Template v1.11 dated 06 01, 2020

Security and Privacy Assessment Plan

Prepared by: [Identify 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: [Identify 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]

Plan Revision History

Date	Description	Version of SAP	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	A=Add M=Modify D=Delete	Description of Change	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]
[1.1	6/1/2020	LL	M	Correction to cover page field	N]

[General Instructions for Completing this Plan:

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

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 SAP.

Instructions for Completing the SAP:

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 information for the scope of the assessment not included 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. After this SAP has been completed, the assessor must meet again with the AE to present the draft SAP and make necessary changes before finalizing the plan. This SAP must be submitted to CMS for review prior to the assessment.]

Table of Contents

List of Tables

1. Introduction

The Administering Entity (AE) [AE Name] [Information System Name] ([Information System Acronym]) will be assessed by [Assessor Name], 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 and Medicaid Services (CMS) provides guidance for employing independent assessors in the Framework for Independent Assessment of Security and Privacy Controls:

> *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 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 Acronym] 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 CMS is required if a system-to-system connection is made to the Federal Data Services Hub (Hub) to exchange data with CMS.

Affordable Care Act (ACA) Administering Entity Systems should also maintain ISAs and Memoranda of Understanding (MOU) between all additional 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)
- 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

1.2 Purpose

This Security and Privacy Assessment Plan (SAP) documents all testing to validate the security and privacy controls for [Information System Acronym]. It has been completed by [Assessor Name] for the benefit of [AE Name]. The Framework for Independent Assessment of Security and Privacy Controls requires:

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

2. Scope

2.1 System or Application Name

[Instructions: 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. Include additional rows as necessary to the tables.

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

Table 1 below indicates 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]

Table 2 below indicates the physical locations of all components that will be assessed.

Table 2. Information System Components

Login URL* Data Center Site Name	Physical Address	Description of Components
[Insert Login URL* Data Center Site name]	[Insert address]	[Insert component description]

** Uniform Resource Locator (URL)*

2.2 IP Addresses Slated for Testing

[Instructions: List the Internet Protocol (IP) addresses of all system components that will be tested. You will need to obtain this information from the SSP and the organization. Note that the IP addresses found in the SSP must be consistent with the boundary. If additional IP addresses are discovered that were not included in the SSP and Privacy Plan, note a finding and advise the organization to update the inventory and boundary information in the SSP. IP addresses can be listed by network ranges and Classless Inter-Domain Routing (CIDR) blocks. If the network is a large network, test a subset of the IP addresses. Include additional rows to the table, as necessary.

The assessor must ensure that the inventory is current before testing and that the inventory and components to be tested are in agreement with the AE. In lieu of filling out this table, the assessor may embed a separate file as long as all required information is included. In addition, the assessor may use any unique identifier (e.g., Media Access Control [MAC] address or hostname), instead of the IP address.

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

Table 3 below indicates the Internet Protocol (IP) addresses and network range of the system that will be tested.

Table 3. IP Addresses Slated for Testing

No.	Item (Manufacturer and Model)	IP Address(s) or Range	Machine /Hostname	Operating System/Software and Version	Function	Item Physical location
[#]	[Insert item manufacturer #]	[Insert IP address or range]	[Insert machine or hostname]	[Insert software and version]	[Insert IP function]	[Insert description of physical network/system? location]

2.3 Applications

[**Instructions:** List all the application that will be tested. You will need to obtain this information from the SSP and the organization.]

Table 4 below indicates the list of applications to be tested.

Table 4. Applications

Vendor	Product Name	Version
[Insert Vendor name]	[Insert product name]	[Insert version #]

2.4 Roles Slated for Testing

[Instructions: Roles to be tested should correspond to those roles listed in the Information System Acronym SSP. Role testing will be performed to test 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.

Delete this, sample tale entries, and all other instructions from your final version of this document.]

Table 5 below indicates the roles that are slated for testing.

Table 5. Roles Slated for Testing

AE Role Name	AE Test User ID/Credential	Assessor Staff Name	Assessor Staff Associated Responsibilities
[Ex. Anonymous Consumer Shopper	Ex. No Account Created	Ex. Jane Doe	Ex. Account Creation]

AE Role Name	AE Test User ID/Credential	Assessor Staff Name	Assessor Staff Associated Responsibilities
[Ex. Agent/Broker Account	Ex. ABTest1	Ex. John Doe	Ex. System Updates]

2.5 Web Applications Slated for Testing

[Instructions: The assessor must test for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Application Security Risks. Provide any web application URL and components that will be in scope for this assessment in the following table. The OWASP Top Ten Most Critical Web Application Security Risks are located at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

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

Table 6 below indicates the web applications slated for testing.

Table 6. Web Applications Slated for Testing

Login URL for the Application	Web Application Name	Function/Description
[Insert login URL]	[Insert web application name]	[Insert description of web application and function]

2.6 Infrastructure and Network Slated for Testing

[Instructions: Identify all infrastructure components that will be in scope for this assessment in the following table.

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

Table 7 below indicates the infrastructure and/or network components slated for testing.

Table 7. Infrastructure and Network Components Slated for Testing

Unique ID	NetBIOS* Name	MAC Address	OS Name and Version	Asset Type	Hardware Make/Model
[#]	[If available, state the NetBIOS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.]	[If available, state the MAC Address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.]	[Operating System Name and Version running on the asset.]	[Simple description of asset function (e.g., Router, Storage Array, and DNS Server)]	[Name of the hardware product and model.]
[Ex. 12	Ex. N/A	Ex. DC-53-60-66-C0-92	Ex. (Community Enterprise Operating System) CentOS 5.1	Ex. Web Server	Ex. ACME Server]

* *Basic Input Output System (BIOS*)

2.7 Databases Slated for Testing

[Instructions: Provide information about databases and instances that will be in scope for this assessment in the following table.

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

Table 8 below indicates the system database(s), instances, and/or tables slated for testing.

Table 8. Databases Slated for Testing

Unique ID	Software/Database Vendor	Software/Database Name and Version	Patch Level	Function
[#]	[Name of Software or Database vendor.]	[Name of Software or Database product and version number.]	[If applicable.]	[For Software or Database, the function provided by the Software or Database for the system.]
[Ex. 13	Ex. Oracle	Ex. Oracle 10g	Ex. 2018.1.1.0000a	Ex. Testing Data]

2.8 Documentation Review

[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 the following required documents as a minimum for the 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 will be assessed:

- Business Agreement with Data Use Agreement (DUA)
- Configuration Management Plan (CMP)
- Contingency Plan (CP) and Test Results
- Plan of Action and Milestones (POA&M)
- System Security and Privacy Plan (SSP), Final
- Incident Response Plan (IRP) and Incident/Breach Notification and Test Plan
- Privacy Impact Assessment (PIA) and other privacy documentation. including, but not limited to, privacy notices and 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 (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
- [Insert additional documents to be reviewed as necessary]

2.9 MARS-E Controls to be Evaluated

[Instructions: The assessor must evaluate the following list of MARS-E security and privacy controls to ensure the effectiveness of the implementation according to the AE SSP workbook. The assessor's evaluation will complement the document review.

The assessor must address the following criteria:

- What controls are tested by the assessor?
- Which MARS-e version is used for testing?

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

The assessor will complete a [full/partial] assessment of the security and privacy controls, using MARS-E version [Insert version number].

[Instructions: In the case of a partial assessment, complete the table below (Table X. Assessed Controls), indicating which controls were assessed, matching the Security and Privacy Assessment Worksheet in Appendix A. Then change font color to black. Ensure to add a table caption with a table number and update all subsequent tables as well as the List of Tables on page iii.

In the case of a full assessment, delete the table below.]

Table X. Assessed Controls

Control Number	Control Name
[AC-1]	[Access Control (AC) Policy and Procedure]
[AC-2]	[Automated System Account Management]

The controls implemented for the [System Acronym] are documented in the [System Acronym] SSP.

2.10 Assumptions/Limitations

[Instructions: The assumptions listed are default assumptions. The assessor must edit these assumptions as necessary for each unique engagement. The assessor may add more assumptions as necessary.

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

1. [AE Name] resources, including documentation and individuals with knowledge of the [AE Name] systems, applications, and infrastructure and associated contact information, will be available to [Assessor Name] assessment staff during the scheduled assessment timeframe and testing activities in order to complete the assessment.
2. The [AE Name] will provide login account information/credentials necessary to perform authenticated scans of devices and applications.
3. The [AE Name] will permit [Assessor Name] assessment staff to connect testing laptops to the [AE Name] networks defined within the scope of this assessment.
4. The [AE Name] 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 Name] personnel will be available should the [Assessor Name] assessment staff determine that either after hours work or weekend work is necessary to support the security and privacy assessment.

3. Methodology

The assessor will perform an assessment of the security and privacy controls using the methodology described in the MARS-E Document Suite and the SSP workbook provided in the Mars-E Volume IV. The results of testing the security requirements will be summarized in the Security and Privacy Assessment Report (SAR) along with the information that notes whether the control is satisfied or not.

3.1 Security and Privacy Controls Assessment Methodology

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 in the MARS-E Volume IV: SSP Template. 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 of the system
- AE policies not followed
- Major documentation omissions and/or discrepancies

3.1.1 Tests and Analyses Performed

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

3.1.2 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 following list includes common test procedures and techniques of the technical assessment:

- Examination of the implemented access controls and identification and authorization techniques (e.g., log-on with easily guessed/default passwords)
- Tests to determine if the system is susceptible to cross-site scripting (XSS), Structured Query Language (SQL) injection, and/or other commonly exploited vulnerabilities
- Attempts to alter database management system settings
- Attempts to access hidden URLs
- Reviews of application-specific audit log configuration settings
- Determination if sensitive information is encrypted before being passed between the system and browser
- Broken Authentication and Session Management
- Sensitive Data Exposure
- XML External Entity (XXE)
- Broken Access Control
- Security Misconfiguration
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

For additional information, consult the Open Web Application Security Project (OWASP) Top Ten Most Critical Web Application Security Risks. Include additional testing scenarios in this subsection response.

3.1.3 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.

3.1.4 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

3.1.5 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 confirms passwords are actually configured as stated in the AE documentation. Core security documentation for review includes documents listed in Table 9 below.

Table 9. Core Security and Privacy Documentation

MARS-E Control Family	MARS-E Control Number	Document Name
Planning (PL)	PL-2: Security System Plan	System Security Plan (SSP)
Configuration Management (CM)	CM-9: Configuration Management Plan	Configuration Management Plan (CMP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing	Contingency Plan (CP) Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	Incident Response Plan (IRP) Test Plan
Awareness and Training (AT)	AT-3: Role-Based Security Training	Security Awareness Training (SAT) Plan
Awareness and Training (AT)	AT-4: Security Training Records	Training Records

MARS-E Control Family	MARS-E Control Number	Document Name
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements (ISA)
Security and Assessment Authorization (CA)	CA-5: Plan of Action and Milestones	Plan of Action and Milestones (POA&M)
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment (PIA) or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the AE privacy risk assessment process, documentation of privacy risk assessments performed by the organization

3.1.6 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 10 below indicates the personnel selected to be interviewed.

Table 10. 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]

Title	Name of Person	Date of Interview	Comments
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]

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

3.1.7 Observations

During the course of the assessment, the assessor will also observe personnel behavior and physical environmental controls, as applicable, to determine if the staff follows 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

The assessor must identify which security configuration benchmarks, including version number, are used (e.g., Defense Information Systems Agency [DISA] Security Technical Implementation Guides [STIGs], United States Government Configuration Baseline [USGCB], etc).

Table 11 below indicates the system and application configuration baselines to be used for this assessment.

Table 11. System/Application Configuration

HW/SW Name	Version	Benchmark	Benchmark Version
[Insert system or application name]	[Insert Version #]	[Ex. DISA, STIGs, or USGCB]	[Insert Benchmark Version #]

[Instructions: The assessor must describe the methodology and process for conducting a complete and accurate security and privacy controls evaluation. The assessor must use Volume IV of the MARS-E Document Suite, which describes the appropriate assessment testing procedure for each control. These test procedures include the test objectives and associated test cases to determine if a control is effectively implemented and operating as intended. The results of the testing will be recorded in the SAR along with information that notes whether the control (or control enhancement) is satisfied or not. The assessor must identify the automated tools that will be used for the assessment, including, but not limited to, tool name, vendor, version, and purpose of the tool. The assessor must identify the manual testing procedures by describing what technical tests will be performed manually without the use of automated tools and how it will be done.

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

[Assessor Name] will perform an assessment of the [Information System Acronym] security and privacy controls using the methodology described in Volume IV of the MARS-E Document Suite. [Assessor Name] will use test procedures to evaluate the security and privacy controls. The testing must include the effectiveness of the most critical security and privacy controls implementation identified by the Center for Internet Security (CIS)[1].

Data gathering activities will consist of the following:

- Request required documentation
- Request any follow-up documentation, files, or information needed that is not provided in required documentation
- Travel onsite as necessary to inspect system or applications and meet with staff
- Obtain information using security testing tools

Security and privacy controls will be verified using one or more of the following assessment methods:

- **Examine:** The assessor will review, analyze, inspect, or observe one or more assessment artifacts as specified in the attached test cases in Appendix A.

[1] Refer to the most current CIS Top Twenty Controls located at: https://www.cisecurity.org/controls/

- **Interview:** The assessor will conduct discussions with individuals within the organization to facilitate Assessor understanding, achieve clarification, or obtain evidence.
- **Technical Tests:** The assessor will perform technical tests, including penetration testing, on system or application components using automated and manual methods.

4. Control Tests and Results

Your active participation is crucial to the successful and timely completion of this assessment. Any slippage (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 in section 6 to ensure availability and communicate any obstacles you foresee. Refer to Appendix A for instructions on how to prepare the Security and Privacy Assessment Worksheet.

4.1 Technical Assessments

[**Instructions:** The assessor must complete the following:

- Test the application or system and the associated infrastructure
- Perform a thorough assessment of the application or system
- Conduct network-based scans of all in-scope network components to determine ports, protocols, and services running on each component
- Review the configurations
- Fill out Table 12 as required]

Table 12 below indicates the tools or procedures used to conduct all scans.

Table 12. Scanning Tools

Test Performed/Purpose	Tools or Procedure	What was Tested
[Ex. Operating System Scan	Ex. Nessus	Ex. Internal boundary complete network]
[Ex. Web Application scan	Ex. HP WebInspect	Ex. Websites]
[Ex. Web Application 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]

4.2 Scanning Authorization

Any scans performed by the assessment team must be approved in advance by the AE Representative. Section 7.6 must be signed by the system owner and forwarded to the assessment team prior to conducting the assessment. This letter will authorize the assessment team to use the tools indicated to perform scans on the [AE Name].

5. Test Roles

5.1 Security and Privacy Assessment Team

[Instructions: List the members of the 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. National Institute of Standards and Technology (NIST) Special Publication 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).

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

The security and privacy assessment team consist of individuals from [Assessor Name], which are located at the following address: [Assessor Name] [Address of Assessor]. Information about [Assessor Name] can be found at the following URL: [Assessor URL].

Table 13 below identifies the members of the assessment team.

Table 13. Security and Privacy Assessment Team

Name	Role	Contact Information
[Insert Assessor name]	[Insert role]	[Insert contact information]

5.2 Provider Testing Points of Contact

[Instructions: The assessor must obtain at least two Points of Contact (POCs) to use for testing communications.

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

Table 14 below identifies the [AE Name] Points of Contact (POCs) that the testing team will use.

Table 14. Provider Testing POCs

Name	Role	Contact Information
[Insert POC name]	[Insert role]	[Insert contact information]

6. Test Schedule

[Instructions: Insert the assessment testing schedule. The following table is a sample and provides suggested tasks and milestones in the assessment process. Assessment tasks may vary between assessments. Remove or add tasks as necessary. 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 make any necessary updates to the schedule and this document and send an updated version to the AE, with copies to the ISSO and the SOP.

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

Table 15 below indicates the assessment testing schedule. All parties must agree on the tasks and durations.

Table 15. Assessment Schedule

Task Name	Start Date	Finish Date
Hold Kickoff Meeting	[Insert start date]	[Insert completion date]
Develop Draft SAP	[Insert start date]	[Insert completion date]
Hold Meeting to Review/Concur upon SAP	[Insert start date]	[Insert completion date]
Finalize SAP	[Insert start date]	[Insert completion date]
Review [Information System Acronym] Documentation	[Insert start date]	[Insert completion date]
Conduct Interviews of [AE Name] Staff:	[Insert start date]	[Insert completion date]
Perform Evaluation/Testing	[Insert start date]	[Insert completion date]
Develop Draft SAR	[Insert start date]	[Insert completion date]
Draft SAR Delivered to AE	[Insert start date]	[Insert completion date]
Hold Issue Resolution Meeting	[Insert start date]	[Insert completion date]

Task Name	Start Date	Finish Date
Finalize SAR	[Insert start date]	[Insert completion date]
Send Final Version of SAR to [AE Name]	[Insert start date]	[Insert completion date]

Table 16 below indicates the schedule of activities and participation for this assessment.

Table 16. Schedule of Activities and Participation

Schedule of 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 • Dates are provided for availability for interviews • 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 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 2 hours. • AE personnel are available for any follow up questions
Reporting	• Assessment Team will be working on the draft SAR • Issue draft SAR by the end of the week	• AE personnel are available for any follow up questions
Finalization/Completion	• Answer any questions on the draft SAR • Schedule and attend debrief if requested • Update final SAR if necessary	• Review draft SAR and provide any comments or schedule debrief within 5 business days

Schedule of Activities	Assessor Responsibilities	AE Personnel Responsibilities
	• Ensure final SAR is issued within 5 business days of debriefing	• Obtain system owner signature on final SAR within 2 days of final issuance

7. Rules of Engagement

[Instructions: 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.

The assessor must edit the ROE as necessary. Both the assessor and AE must sign the final version of the ROE.

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

7.1 Disclosures

[Instructions: Edit and modify the 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.

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

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. All scans will originate from the following IP address(es): [List IP addresses for Scan Test].

7.2 Test Inclusions

[Instructions: The assessor must edit the bullets in this default list of test inclusions to make it consistent with each unique system tested.

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

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
- [Insert additional test inclusions here]

7.3 Test Exclusions

[Instructions: The assessor must edit the bullets in this default list of test exclusions to make it consistent with each unique system tested.

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

Security testing will not include any of the following activities:

- Changes to assigned user passwords
- Modification of user files or system files
- Telephone modem probes and scans (active)
- Intentional viewing of [AE Name] staff email, Internet caches, and/or personnel cookie files
- Denial of service attacks
- Exploits that will introduce new weaknesses to the system
- Intentional introduction of malicious code (viruses, trojans, worms, etc.)
- [Insert additional test exclusions here]

7.4 End of Testing

[Assessor Name] will notify the designated [AE Name] 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] requirements. Security testing results will be sent and disclosed to the individuals at [AE Name] within [#] days after security test has been completed.

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

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

In the status column, an indication on 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 the [Assessor Name] and [AE Name] have been identified as having the authority to agree to security testing of [Information System Acronym]. 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.

[Assessor Name] Representative		[AE Name] Representative	
(Name)		(Name)	
(Signature)	(Date)	(Signature)	(Date)

Appendix A. Security and Privacy Assessment Worksheet

The assessor will use the Security and Privacy Assessment Worksheet located at https://zone.cms.gov/document/ae-security-and-privacy-assessment-plan-sap to prepare for the Security and Privacy Control Assessment. The pre-filled out worksheet will be included in a zip file along with this assessment plan.

[Instructions: Prepare the Security and Privacy Assessment Worksheet located in zONE (Example 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: Identify artifacts and processes that will be examined for each control.

Test Methods and Objects: Identify methods and objects you will use to test each control. If automated tools are utilized for this assessment, identify which tools were utilized.

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

Result (Pass): N/A. To be filled out after assessment is completed.

Result (Fail): N/A. To be filled out after assessment is completed.

Comments: Include comments as needed.

NOTE: If a control is N/A, indicate why it is N/A in the Comments section.

Include the pre-filled out worksheet in a zip file along with the SAP.

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

Appendix B. Penetration Testing and Methodology

[Instructions: Penetration testing is currently optional. If performed, the Assessor must attach a file containing the plan or include the plan in this Appendix. The penetration testing must include, in part, the security testing scenarios found in subsection 3.1.2.

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

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

Appendix C. 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