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

Sensitive and Confidential Information – For Official Use Only

Non-Exchange Entity Name (Acronym)

Security and Privacy Controls Assessment Test Plan of the <Name of NEE>

<Name of NEE Information System>

As performed by <Auditor Company Name>

SAP Version 0.1

Report Publication Date

CMS SAP Template v 3.1

Security and Privacy Controls Assessment Test Plan

Prepared by: <Identify Auditor that prepared this document>

Organization Name: <Enter Company/Organization>.
Street Address: <Enter Street Address>
Suite/Room/ Building: <Enter Suite/Room/Building>
City, State Zip: <Enter Zip Code>

Prepared for: <Name of NEE>

Organization Name: <Enter Company/Organization>.
Street Address: <Enter Street Address>
Suite/Room/ Building: <Enter Suite/Room/Building>
City, State Zip: <Enter Zip Code>

Revision History

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

Instruction

(Delete page when draft plan is completed.)

The assessment test plan must be jointly completed and agreed to before the start of the assessment by both the Enhanced Direct Enrollment (EDE) Entity and the Auditor. To expedite the process, this may be done during an assessment kickoff meeting.

It is strongly recommended that Non-Exchange Entities (NEE) that are not EDE Entities contract with a third-party auditor that has experience conducting information system privacy and security audits to perform the assessment. This Security and Privacy Controls Assessment Test Plan (SAP) provides the template that the auditor should use for the assessment.

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 Auditor must obtain this to accurately complete the assessment plan.

The NEE 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 plan has been completed, the Auditor must meet again with the NEE to present the draft security assessment plan and make necessary changes before finalizing the plan. This Security and Privacy Controls Assessment Test Plan (SAP) must be submitted to CMS for review prior to the assessment.

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

Table of Contents

List of Tables

1. Introduction

The <Information System Name> (<Information System Abbreviation>) will be assessed by <Auditor Name>, the Auditor. This Security and Privacy Controls Assessment Test Plan (SAP) must be submitted to the Centers for Medicare & Medicaid Services (CMS) for review prior to the assessment. Both EDE Entities[1] and Non-Exchange Entities (NEEs) participating in the classic Direct Enrollment program only (e.g., Web-Brokers not participating in the EDE program) should have a fully completed and implemented System Security and Privacy Plan (SSP) prior to starting the security and privacy audit.

The use of an independent assessment team reduces the potential for conflicts of interest that could occur in verifying the implementation status and effectiveness of the security controls. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk* states:

> Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of security and privacy control effectiveness. The Auditor's role is to provide an independent assessment of the compliance of the enhanced direct enrollment pathway and to maintain the integrity of the audit process. The Auditor is required to attest to their independence and objectivity in completing the audit, and that neither the NEE nor the Auditor took any actions that might impair the objectivity of the findings in the audit in Section 6.7.

1.1 Applicable Laws, Regulations, and Standards

By interconnecting with the CMS network and CMS information system, the <Name of NEE> agrees to be bound by the Interconnection Security Agreement (ISA) and the use of the CMS network and information system in compliance with the ISA. Laws, regulations, and standards that apply include the following:

- Federal Information Security Management Act of 2014 (FISMA)
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
- 18 U.S.C. § 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information
- Privacy Act of 1974, 5 U.S.C. § 552a
- Health Insurance Portability and Accountability Act (HIPAA) of 1966 P.L. 104-191
- Patient Protection and Affordability Care Act ("PPACA") of 2010

[1] Enhanced Direct Enrollment (EDE) Entities are considered NEEs and will be referred to as NEEs in this document.

- HHS Regulation 45 CFR §155.260 – Privacy and Security of Personally Identifiable Information
- HHS Regulation 45 CFR §155.280 – Oversight and monitoring of privacy and security requirements
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*

1.2 Purpose

This *Security and Privacy Controls Assessment Test Plan* documents all testing to be conducted during the assessment to validate the security and privacy controls for <Information System Abbreviation>. It has been completed by <Auditor Name> for the benefit of <Name of NEE>. NIST SP 800-39, *Managing Information Security Risk* states:

> The information system owner and common control provider rely on the security expertise and the technical judgment of the assessor to: (i) assess the security controls employed within and inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

2. Scope

2.1 System or Application Name

Instruction: 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 System Security and Privacy Plan (SSP).

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

Include additional rows as necessary to the tables.

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

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

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

Table 1 describes 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 describe the physical locations of all components that will be tested.

Table 2. Information System Components

Login URL* Data Center Site Name	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

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

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

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

Table 3 identifies the 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 Roles Slated for Testing

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

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

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

For this assessment, <Auditor Name> staff names have been associated with the specific roles and corresponding responsibilities.

Table 4 identifies the roles slated for testing.

Table 4. Roles Slated for Testing

NEE Role Name	NEE Test User ID/Credential	Auditor Staff Name	Auditor Staff Associated Responsibilities
[Ex. Anonymous Consumer Shopper]	[Ex. No Account Created]	[Ex. Jane Doe	[Ex. Account Creation]
[Ex. Agent / Broker Account]	[Ex. ABTest1]	[Ex. John Doe	[Ex. System Updates]

2.4 Applications Slated for Testing

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

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

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

Table 5 below indicates the list of applications to be tested.

Table 5. Applications

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

2.5 Web Applications Slated for Testing

Instruction: The Auditor must test for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Application Security Risks.[2] Provide any web application URL and components that will be in scope for this assessment in the following table.

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

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

Table 6 identifies 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

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

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

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

Table 7 identifies the infrastructure and/or network components of the system that will be tested.

[2] The OWASP Top Ten Most Critical Web Application Security Risks are located at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

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 the asset's 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. CentOS 5.1]	[Ex. Web Server]	[Ex. Acme Server]

2.7 Databases Slated for Testing

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

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

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

Table 8 identifies the system database(s), instances, and/or tables that will be tested.

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

Instruction: Security and privacy documentation will be reviewed for completeness and accuracy. Through this process, the Auditor will gain insight to determine if all controls are implemented as described. The Auditor's review also augments technical control testing.

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

If any document is removed, please provide an alternative document or explanation as to why.

[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 PII and Privacy Act Statements
- Security Awareness Training (SAT) Plan and Training Records
- Interconnection Security Agreements (ISA)
- Information Security Risk Assessment (ISRA)
- Governance documents and privacy policy

2.9 NEE SSP Controls to Be Tested

Instruction: The Auditor must test all security and privacy controls in the NEE SSP workbook to ensure the effectiveness of the implemented controls. The Auditor's testing will complement the document review.

Note: Auditors must test the Concurrent Session Control and Remote Access use cases as documented in the EDE Auditor Guidelines.

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

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

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

The controls implemented for the <Information System Abbreviation> can be found documented in the <Information System Abbreviation> SSP.

[Instructions: The assessor must evaluate the following list of NEE security and privacy controls to ensure the effectiveness of the implementation according to the NEE 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 NEE guidance 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 NEE plan year [Insert year].

[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.

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

Table 9. Assessed Controls

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

Control Number	Control Name

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

2.10 Assumptions / Limitations

Instruction: The assumptions listed are default assumptions. The Auditor must edit these assumptions as necessary for each unique engagement. The Auditor may add more assumptions as necessary.

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

1. <Name of NEE> resources, including documentation and individuals with knowledge of the <Name of NEE> systems, applications, and infrastructure and associated contact information, will be available to <Auditor Name> assessment staff during the scheduled assessment timeframe and testing activities in order to complete the assessment.
2. The <Name of NEE> will provide login account information/credentials necessary for <Auditor Name> assessment staff to use with its testing devices to perform authenticated scans of devices and applications.
3. The <Name of NEE> will permit <Auditor Name> assessment staff to connect testing laptops to the <Name of NEE> > networks defined within the scope of this assessment.
4. The <Name of NEE> will permit communication from the Auditor testing appliances to an internet-hosted vulnerability management service to permit the analysis of vulnerability data.
5. Security 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 security controls.
6. Significant upgrades or changes to the infrastructure and components of the system undergoing testing will not be performed during the security assessment period.
7. For onsite control assessment, <Name of NEE> personnel will be available should the <Auditor Name> assessment staff determine that either after hours work or weekend work is necessary to support the security assessment.

3. Methodology

Instruction: The Auditor must describe the methodology and process for conducting a complete and accurate security and privacy controls testing. The Auditor must use NIST SP 800-53A 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 Security and Privacy Assessment Report (SAR) along with information that notes whether the control (or control enhancement) is satisfied or not.

The Auditor 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 Auditor 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. The Auditor must identify which security configuration benchmarks, including version number, are used (e.g., DISA STIGs, and USGCB).

Complete Table 10, Table 11, Table 12, and Table 13 as required.

The Auditor may edit this section as appropriate.

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

<Auditor Name> will perform an assessment of the <Information System Abbreviation> security and privacy controls using the methodology described in NIST SP 800-53A. <Auditor Name> will use test procedures to evaluate the security and privacy controls. The testing must include the effectiveness of the most critical security controls implementation identified by the Center for Internet Security.[3]

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 Auditor will review, analyze, inspect, or observe one or more assessment artifacts as specified in the attached test cases in Appendix A.

[3] Please refer to the most current CIS Top Twenty Controls located at: https://www.cisecurity.org/controls/. Also, CMS has provided a mapping of the NEE SSP controls to the CIS Top Twenty Controls.

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

[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
- Complete Table 10, Table 11, Table 12, and Table 13 as required.
- If N/A is provided, please provide a detailed explanation as to why.

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

Table 10. 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 #]

Table 11. 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]

Table 12. 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]

Title	Name of Person	Date of Interview	Comments
Contingency Planning Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Database Administrator	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Data Center Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Facilities Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Firewall Administrator	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Human Resources Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Information System Security Officer	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Privacy Program Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Privacy Officer	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Media Custodian	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Network Administrator	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Program Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
System Administrators	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
System Owner	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]
Training Manager	[Insert name of individual]	[Insert interview date]	[Identify any further relevant information]

Table 13. Manual Testing Procedures

Test ID #	Test	Manual Testing Procedure	Comments
1	[Test]	[Insert testing procedure]	[Identify any further relevant information]
2	[Test]	[Insert testing procedure]	[Identify any further relevant information]
3	[Test]	[Insert testing procedure]	[Identify any further relevant information]

4. Test Roles

4.1 Security and Privacy Assessment Team

Instruction: 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. NIST SP 800-39, *Managing Information Security Risk* states:

> The security control 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).

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

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

The security and privacy assessment team consists of individuals from <Auditor Name>, which are located at the following address: <Auditor Name> < Address of Auditor>. Information about <Auditor Name> can be found at the following URL: <Auditor URL>.

Table 14 presents the members of the Auditor assessment team.

Table 14. <Auditor Name> Security and Privacy Assessment Team

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

4.2 Provider Testing Points of Contact

Instruction: The Auditor must obtain at least two points of contact to use for testing communications.

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

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

Table 15 lists the <Name of NEE> points of contact that the testing team will use.

Table 15. Provider Testing Points of Contact

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

5. Test Schedule

Instruction: 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 NEE by the Auditor 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 NEE. After the Auditor presents the testing schedule to the NEE at the kickoff meeting, the Auditor must make any necessary updates to the schedule and this document and send an updated version to the NEE, with copies to the ISSO and the SOP.

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

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

Table 16 presents the assessment testing schedule. All parties must agree on the tasks and durations.

Table 16. Test 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 SAP	[Insert start date]	[Insert completion date]
Finalize SAP	[Insert start date]	[Insert completion date]
Review <Information System Abbreviation> Documentation	[Insert start date]	[Insert completion date]
Conduct Interviews of <Name of NEE> Staff	[Insert start date]	[Insert completion date]
Perform Testing	[Insert start date]	[Insert completion date]
Develop Draft SAR	[Insert start date]	[Insert completion date]
Draft SAR Delivered to NEE	[Insert start date]	[Insert completion date]
Hold Issue Resolution Meeting	[Insert start date]	[Insert completion date]
Finalize SAR	[Insert start date]	[Insert completion date]
Send Final Version of SAR to <Name of NEE>	[Insert start date]	[Insert completion date]

Table 17 below is a *suggested* schedule of activities and participation for this assessment.

Table 17. Schedule of Activities and Participation

Schedule of Activities	Assessor Responsibilities	NEE 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 NEE 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 • NEE tester POC is available for any issues (account reset, connectivity loss, etc). Response time should be within 2 hours. • NEE 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	• NEE 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 • Obtain system owner signature on final SAR

Schedule of Activities	Assessor Responsibilities	NEE Personnel Responsibilities
	• Ensure final SAR is issued within 5 business days of debriefing	within 2 days of final issuance

6. Rules of Engagement

Instruction: The RoE describes proper notifications and disclosures between the owner of the systems or applications being tested and the Auditor. A 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 Auditor must edit the Rules of Engagement (RoE) as necessary. The final version of the RoE must be signed by both the Auditor and NEE must sign the final version of the RoE.

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

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

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

6.1 Disclosures

Instruction: 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 NEE will understand that the rapid and high-volume network traffic is not an attack and is part of the testing performed by the Auditor.

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

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

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>.

6.2 Security Testing Scenarios

Instruction: The following Vulnerabilities and Testing scenarios are provided by CMS and their testing is required:

Test specifically for the following security vulnerabilities in addition to the security controls provided:

1. SQL Injection

2. Broken Authentication and Session Management
3. Sensitive Data Exposure
4. XML External Entity (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

For additional information, consult the OWASP Top Ten Most Critical Web Application Security Risks. Please include additional testing scenarios in this subsection response.

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

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

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

6.3 Test Inclusions

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

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

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

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 structured query language (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

6.4 Test Exclusions

Instruction: The Auditor must edit the bullets in this default list of test exclusions to make it consistent with each unique system tested. Insert additional test exclusions here if applicable.

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

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

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 <Name of NEE> 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 if applicable]

6.5 End of Testing

<Auditor Name> will notify <Name of NEE> when security testing has been completed.

6.6 Communication of Test Results

Email and reports on all security testing will be encrypted according to <Name of NEE> requirements. Security testing results will be sent and disclosed to the individuals at <Name of NEE> within <number> 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.

6.7 Signatures

The following individuals at the <Auditor Name> and <Name of NEE> have been identified as having the authority to agree to security testing of <Information System Abbreviation>. The Auditor attests to their independence and objectivity throughout the security and privacy assessment.

The following individuals acknowledge the foregoing Security and Privacy Assessment Plan and Rules of Engagement and agree to the tests and terms set forth in the plan.

<Auditor Name> Representative	<Name of NEE> Representative
(Name)	(Name)
(Signature) (Date)	(Signature) (Date)

Appendix A. Test Case Procedures

Instruction: The Auditor must provide the test procedures containing the test objectives and associated test cases to determine if a control is effectively implemented and operating as intended. The Auditor can provide the test case procedures in an Excel worksheet.

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

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

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

Appendix B. Penetration Testing and Methodology

Instruction: The Auditor 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 6.2. References to websites for their penetration testing and methodology will not be accepted.

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

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

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

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