security requirements will be summarized in the SAR along with the information that notes whether the control is satisfied or not.

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

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

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

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

## 6.2 Tests and Analysis Performed

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

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

## 6.3 Security and Privacy Controls Technical Testing

Typically, the assessment staff provides user access to the system to conduct the application or system security technical testing. To perform a thorough assessment of the application or system, application-specific user accounts that reflect the different user types and roles are created for the

## 8.6 Signatures

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

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

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

# Appendix A. Penetration Testing

<<The Assessor must attach a file containing the Penetration Test Plan or include the plan in this Appendix. Penetration testing must include, in part, the security testing scenarios found in Section 6.3.

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

In the brackets enter either "below" or "the attached document".>>

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

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

# Appendix B. 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 |
| CA | Security Assessment and Authorization, a Security Control family |
| CIA | Confidentiality, Integrity, and Availability |
| C.F.R. | Code of Federal Regulation |
| CIDR | Classless Inter-Domain Routing |
| CM | Configuration Management, a Security Control family |
| CMP | Configuration Management Plan |
| CMS | Centers for Medicare & Medicaid Services |
| CP | Contingency Planning, a Security Control family |
| DUA | Data Use Agreement |
| FISMA | Federal Information Security Management Act |
| FTI | Federal Tax Information |
| HHS | Department of Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| Hub | Federal Data Services Hub |
| IR | Incident Response, a Privacy Control family |
| IRP | Incident Response Plan |
| ISA | Interconnection Security Agreement |
| 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 |
| PHI | Protected Health Information |
| PIA | Privacy Impact Assessment |

| | |
|---|---|
| PII | Personally Identifiable Information |
| PL | Planning, a Security Control family |
| PL | Public Law |
| POA&M | Plan of Action & Milestones |
| POC | Point of Contact |
| RA | Risk Assessment, a Security Control family |
| ROE | Rules of Engagement |
| SAP | Security and Privacy Assessment Plan |
| SAR | Security and Privacy Assessment Report |
| SAT | Security Awareness Training |
| SAW | Security and Privacy Assessor Workbook |
| SCA | Security and Privacy Controls Assessment |
| SME | Subject Matter Expert |
| SOP | Senior Official for Privacy |
| SP | Special Publication |
| SQL | Structured Query Language |
| SSP | System Security and Privacy Plan |
| URL | Uniform Resource Locator |
| USC | United States Code |
| XSS | Cross-Site Scripting |
| XXE | XML External Entity |