

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244-1850



*Annual Security and Privacy Attestation
Procedures
for the Affordable Care Act
Information Systems*

Final

February 2016

Version 2.0

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Record of Changes

Number	Date	Reference	A=Add, M=Modify, D=Delete	Description of Change	Change Request #
Version 1.0	10/2014			Final draft	
Version 2.0	03/2016		A	Final Draft (Privacy Updates)	

Table of Contents

1. INTRODUCTION	1
1.1 Requirements Background.....	1
1.2 Purpose.....	1
2. ANNUAL SECURITY AND PRIVACY ATTESTATION.....	1
2.1 Annual Security and Privacy Attestation Process.....	2
2.2 Attestation Testing.....	3
2.3 Annual Security and Privacy Attestation Report.....	3
2.4 Submission Timeframe	4
APPENDIX A Annual Security and Privacy Attestation Report Template	5

1. INTRODUCTION

The Annual Security and Privacy Attestation Procedures for the Affordable Care Act (ACA) Information Systems provides guidance and the report template for the annual attestation of the Minimum Acceptable Risk Standards for Exchanges (MARS-E) security and privacy controls mandated by the Centers for Medicare & Medicaid Services (CMS). The annual attestation is one of the activities associated with the security control continuous monitoring process and the privacy controls including privacy impact, risk assessment, monitoring, and auditing.

1.1 REQUIREMENTS BACKGROUND

The basis for the annual security and privacy attestation is the MARS-E 2.0 Security Assessment Control (CA-2). This control requires that all MARS-E security and privacy controls, attributable to a specific system or application, be assessed over a three-year period with a subset of the controls assessed annually during the annual attestation process. Additionally, the MARS-E Continuous Monitoring Control (CA-7) requires organizations to implement a continuous monitoring program that includes reporting of the security state of the information system to appropriate organizational officials every 365 days. The enforcement of these controls supports the identification of significant security vulnerabilities by recognizing non-compliant control areas in a timely manner. The MARS-E Privacy Impact and Risk Assessment Control (AR-2) is also part of this annual review.

The assessment and resulting attestation report provided to CMS help identify and address systemic security and privacy issues and provides a detailed understanding of the current security and privacy posture associated with the broader ACA program.

1.2 PURPOSE

This document provides guidance and direction for:

- Ensuring ACA systems comply with MARS-E
- Testing at least one-third of the MARS-E security controls annually
- Testing privacy controls
- Reviewing and updating ACA systems security and privacy documentation
- Completing and submitting the Annual Security and Privacy Attestation Report

2. ANNUAL SECURITY AND PRIVACY ATTESTATION

The annual security and privacy control attestation may be conducted by the Administering Entity (AE) business owner, the system owner, the system developer/maintainer, or by an independent assessor. If an independent assessor performs the testing for the annual attestation, the test results are documented in a Security and Privacy Assessment Report (SAR). This report can be applied to the triennial security and privacy control testing necessary for the renewal of an Authority to Connect (ATC).

2.1 ANNUAL SECURITY AND PRIVACY ATTESTATION PROCESS

The annual security and privacy attestation process includes the following activities by the AE:

- Review the AE’s policies and procedures and attest to their implementation
- Determine security and privacy controls to be tested including:
 - Control families for current year (See Appendix A instructions)
 - Controls to be tested annually (See Appendix A instructions)
 - Controls with identified weaknesses closed during the current year (*Note: completed/closed findings on the Plan of Action and Milestones (POA&M) should remain on the POA&M 1 year*)
 - Controls impacted by changes to the system environment during the current year
- Review and evaluate ACA security and privacy documentation by the Administering Entity. The assessment and resulting attestation report must be submitted to CMS.
 - Information Security Risk Assessment (ISRA) to determine:
 - Significant changes to business objectives or overall mission importance
 - Significant changes to the security state due to new or modified federal legislation, regulations, directives, policies, standards, or guidance
 - Effectiveness of security controls changed during the past year
 - New vulnerabilities affecting the overall risk to the system found during continuous monitoring activities, the annual security and privacy attestation process, and the independent security assessment process
 - System Security Plan (SSP) including the security and privacy implementations to verify the system information and control implementation documented is correct and updated as necessary
 - Contingency Plan (CP) and the Annual CP Test with the following:
 - Validate the Maximum Tolerable Disruption (MTD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
 - Test and exercise the CP using the CP Test Plan
 - Document the results of the CP test in a report
 - Update the CP based on the test results
- Review the Privacy Impact Assessment (PIA) to verify that privacy controls are documented, privacy risks are assessed, and control implementations have not changed
- Review legal agreements with CMS and other business partners to ensure they are current. These agreements include:
 - Interconnection Security Agreement (ISA)
 - Computer Matching Agreement (CMA)
 - Information Exchange Agreement (IEA)
 - Other forms of agreements such as data use agreements

2.2 ATTESTATION TESTING

The AE may fulfill the annual attestation requirement by using the current year's security and privacy control assessment results from any of the following sources, including but not limited to:

- An independent assessment
- Assessments conducted as part of an ATC or reauthorization
- Continuous monitoring activities
- Ongoing testing and evaluation of security and privacy associated with the system development life cycle
- Internal privacy risk assessments and audits from the Office of the Inspector General (OIG), the General Accounting Office (GAO), or the Internal Revenue Service (IRS)

Depending on the extent of testing from other sources, the organization may need to perform additional testing to ensure all security controls are reviewed and validated against the MARS-E required controls. For testing the controls, the procedures for each control are documented in MARS-E.

The use of automated support tools (e.g. vulnerability scanners, patch management and configuration management software solutions) facilitates near real-time risk management by tracking violation and compliance changes. These types of tools and the associated reporting performed can assist the AE in validating the adequacy of security and privacy control implementations.

Only security control testing after June 30 of the prior year will be attributed to the current year's annual attestation.

2.3 ANNUAL SECURITY AND PRIVACY ATTESTATION REPORT

The template provided in Appendix A must be used to complete the annual security and privacy attestation. The signatories on the report personally attest to the report's accuracy and authenticity.

In addition to the information to be completed for the controls, the summary section of the report requires the latest review date for the following security documents:

- System Security Plan and supporting Attachments
- Information Security Risk Assessment
- Contingency Plan
- Contingency Plan Test Date
- PIA
- POA&Ms
- Legal Agreements such as the Computer Matching Agreement (CMA) or the Information Exchange Agreement (IEA)

2.4 SUBMISSION TIMEFRAME

The Annual Security and Privacy Attestation Report is due to CMS no later than June 30th of each year or the last workday prior, whichever is sooner.

APPENDIX A: Annual Security and Privacy Attestation Report Template

Instructions for Completing the Annual Security and Privacy Attestation Report

1. Modify the AE in all locations to reflect the entity for which the report is being submitted
2. Update to reflect the year being reported: Self- Attestation for Year: (ex. June 2015 – June 2016)
3. Update to reflect the actual completion date: Date Completed: (ex. June 30, 2016)
4. Change date in Footer of checklist
5. Complete Attestation Summary Report

Check either **Met or Not Met** and complete the date that the activity was completed or verified.

6. Complete security control review table:

1. Test Year Column

ALL – Controls designated as critical are required to be tested every year (**BOLDED**). The PIA, which is assessed annually, provides documentation for most of the Privacy Controls, therefore, the privacy controls are tested every three years as part of the ATC full assessment.

Y1 – Controls to be tested during the first year attestation

Y2 – Controls to be tested during the second year attestation

Y3 – Controls to be tested during the third year attestation

Control & Control Name Columns

The control identifier and the control title as noted in the MARS-E Control Catalog.

Year (Y1) testing:

- Access Controls (AC)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Physical and Environmental Protection (PE)
- Personnel Security(PS)
- System and Communications Protection (SC)

Year (Y2) testing:

- Access Controls
- Audit and Accountability (AU)
- Configuration Management
- Contingency Planning (CP)
- Security Planning (PL)
- Program Management(PM)
- Risk Assessment (RA)

- System Integrity (SI)

Year (Y3) testing:

- Access Controls
- Configuration Management
- Awareness and Training (AT)
- Security Assessment and Authorization (CA)
- Incident Response (IR)
- System Maintenance (MA)
- Media Protection (MP)
- System and Services Acquisition (SA)

Critical Controls (policies and procedures) reviewed and updated each year:

- Access Control Policy and Procedures
- Account Management
- Security Awareness and Training Policy and Procedures
- Audit and Accountability Policy and Procedures
- Security Assessment and Authorization Policies and Procedures
- Security Assessments
- Configuration Management Policy and Procedures
- Contingency Planning Policy and Procedures
- Identification and Authentication Policy and Procedures
- Incident Response Policy and Procedures
- System Maintenance Policy and Procedures
- Media Protection Policy and Procedures
- Physical and Environmental Protection Policy and Procedures
- Security Planning Policy and Procedures
- Personnel Security Policy and Procedures
- Risk Assessment Policy and Procedures
- System and Services Acquisition Policy and Procedures
- System and Communication Protection Policy and Procedures
- System and Information Integrity Policy and Procedures
- Information Security Program Plan

Additional controls tested each year (ALL):

- AT-2 Security Awareness Training
- AT-3 Role-Based Security Training
- AT-4 Security Training Records
- AU-2 Audit Events
- CA-2 Security Assessments

- CP-2 Contingency Plan
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing
- CP-9(1) Testing for Reliability/Integrity
- IA-2 Identification and Authentication (Organizational Users)
- IA-5 Authenticator Management
- IR-2 Incident Response Training
- IR-3 Incident Response Testing
- IR-8 Incident Response Plan
- MP-6(2) Equipment Testing
- PE-3 Physical Access Control
- PL-2 System Security Plan
- PL-4 Rules of Behavior
- PS-2 Position Risk Designation
- PS-6 Access Agreements
- RA-3 Risk Assessment
- RA-5 Vulnerability Scanning
- SA-3 System Development Lifecycle
- SC-5 Denial of Service Protection
- SC-7 Boundary Protection
- SC-8 Transmission Confidentiality and Integrity
- SC-13 Cryptographic Protection
- SC-ACA-1 Electronic Mail
- SC-ACA-2 FAX Usage
- SI-2 Flaw Remediation
- SI-4 Information System Monitoring
- SI-7 Software, Firmware, and Information Integrity
- SI-10 Information Input Validation
- AR-2 Privacy Impact Assessment

2. Test Result Column

Note the test results:

- Passed -All requirements of the control have been met and tested successfully
- Failed - All requirements of the control have not been met and test was not successful

3. Type of Test/Audit Column

Test/Audit Type:

- **AA** – Annual security and privacy attestation test
- **ATC**- Assessments for ATC or reauthorization
- **CM** - Continuous monitoring activities
- **ELC Test** -Ongoing testing and evaluation of information system security and privacy throughout the development life cycle
- **TIA** – Three-Year Independent Assessment
- **AUDIT** – Results of state audits (to support independent assessments)

4. Date Tested Column

Note the date the control test was completed

5. POA&M Identifier Column

Note the POA&M identifier number and risk level assigned

6. Sample Completed Row

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
All	AC-1	Access Control Policy and Procedures	<i>Passed</i>	<i>AA Annual Attestation</i>	<i>YR2 June 1, 2015</i>	<i>If a weakness, place the Identifier here (e.g. AC-1 + local POA&M # designation)</i>

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Annual Security and Privacy Attestation Report – *State-Based Administering Entity*

Self-Attestation for Year: (e.g. June 2015 – June 2016)

Date Completed: (e.g. June 30, 2016)

Attestation Identification	
State-Based Administering Entity	XXX
System Name	XXX
Business Owner	XXX
Security Officer	XXX
Privacy Officer	XXX

Attestation Summary Report	Met	Not Met	Date (Day/Month/Year)
1. Authority to Connect			
Expiration Date			
2. Review organization continuous monitoring policies and procedures and attest to adherence			
3. Risk Assessments Reviewed and Updated			
4. System Security Plan including Security and Privacy Control Implementations Reviewed/ Updated			
5. Security and/or Privacy Control Assessment Completed (Note: Y1, Y2, or Y3.			
A. One third of MARS-E controls (Yes or No) Annual Assessment Checklist Completed and Attached			
B. All controls (Yes or No) Independent Assessment- Security and Privacy Assessment Report attached			
6. Contingency Plan Reviewed and Updated			
7. Contingency Plan Tested			
8. PIA Reviewed and Updated			
9. POA&Ms Reviewed and Updated			

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Attestation Summary Report	Met	Not Met	Date (Day/Month/Year)
10. CMA agreement is current			
11. IEA agreement is current			
12. ISA agreement is current			

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	AC-1	Access Control Policy and Procedures				
ALL	AC-2	Account Management				
ALL	AC-2(1)	Automated Information System Account Management				
ALL	AC-2(2)	Removal of Temporary/Emergency Accounts				
ALL	AC-2(3)	Disable Inactive Accounts				
ALL	AC-2(4)	Automated Audit Actions				
ALL	AC-2(7)	Role-Based Schemes				
ALL	AC-3	Access Enforcement				
ALL	AC-3(9)	Access Enforcement - Controlled Release				
ALL	AC-4	Information Flow Enforcement				
ALL	AC-5	Separation of Duties				
ALL	AC-6	Least Privilege				
ALL	AC-6(1)	Authorize Access to Security Functions				
ALL	AC-6(2)	Non-Privileged Access for Non-Security Functions				
ALL	AC-6(5)	Privileged Accounts				
ALL	AC-6(9)	Auditing Use of Privileged Functions				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions				
ALL	AC-7	Unsuccessful Login Attempts				
ALL	AC-8	System Use Notification				
ALL	AC-10	Concurrent Session Control				
ALL	AC-11	Session Lock				
ALL	AC-11(1)	Pattern-Hiding Displays				
ALL	AC-12	Session Termination				
ALL	AC-14	Permitted Actions Without Identification Or Authentication				
ALL	AC-17	Remote Access				
ALL	AC-17(1)	Automated Monitoring/Control				
ALL	AC-17(2)	Protection of Confidentiality/Integrity Using Encryption				
ALL	AC-17(3)	Managed Access Control Points				
ALL	AC-17(4)	Privileged Commands/Access				
ALL	AC-18	Wireless Access				
ALL	AC-18(1)	Authentication and Encryption				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	AC-19	Access Control for Mobile Devices				
ALL	AC-19(5)	Full-Device / Container-Based Encryption				
ALL	AC-20	Use of External Information Systems				
ALL	AC-20(1)	Limits on Authorized Use				
ALL	AC-20(2)	Portable Storage Devices				
ALL	AC-21	Information Sharing				
ALL	AC-22	Publicly Accessible Content				
ALL	AT-1	Security Awareness and Training Policy and Procedures				
ALL	AT-2	Security Awareness Training				
Y3	AT-2(2)	Insider Threat				
ALL	AT-3	Role-Based Security Training				
ALL	AT-4	Security Training Records				
ALL	AU-1	Audit and Accountability Policy and Procedures				
ALL	AU-2	Audit Events				
ALL	AU-2(3)	Reviews and Updates				
Y2	AU-3	Content of Audit Records				
Y2	AU-3(1)	Additional Audit Information				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y2	AU-4	Audit Storage Capacity				
Y2	AU-5	Response To Audit Processing Failures				
Y2	AU-5(1)	Audit Storage Capacity				
Y2	AU-6	Audit Review, Analysis, and Reporting				
Y2	AU-6(1)	Process Integration				
Y2	AU-6(3)	Correlate Audit Repositories				
Y2	AU-7	Audit Reduction and Report Generation				
Y2	AU-7(1)	Automatic Processing				
Y2	AU-8	Time Stamps				
Y2	AU-8(1)	Synchronization with Authoritative Time Source				
Y2	AU-9	Protection of Audit Information				
Y2	AU-9(4)	Access by Subset of Privileged Users				
Y2	AU-10	Non-Repudiation				
Y2	AU-11	Audit Record Retention				
Y2	AU-12	Audit Generation				
Y2	AU-12(1)	System-Wide/Time-Correlated Audit Trail				
Y2	AU-16	Cross-Organizational Auditing				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	CA-1	Security Assessment and Authorization Policies and Procedures				
ALL	CA-2	Security Assessments				
Y3	CA-2(1)	Independent Assessors				
Y3	CA-3	System Interconnections				
Y3	CA-3(5)	Restrictions on External System Connections				
Y3	CA-5	Plan of Action and Milestones				
Y3	CA-5(1)	Automation Support for Accuracy/Currency				
Y3	CA-6	Security Authorization				
Y3	CA-7	Continuous Monitoring				
Y3	CA-7(1)	Independent Assessment				
Y3	CA-9	Internal System Connections				
ALL	CM-1	Configuration Management Policy and Procedures				
ALL	CM-2	Baseline Configuration				
ALL	CM-2(1)	Reviews and Updates				
ALL	CM-2(3)	Retention of Previous Configurations				
ALL	CM-3	Configuration Change Control				
ALL	CM-3(2)	Test/Validate/Document Changes				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	CM-4	Security Impact Analysis				
ALL	CM-4(1)	Separate Test Environments				
ALL	CM-4(2)	Verification of Security Functions				
ALL	CM-5	Access Restrictions for Change				
ALL	CM-5(1)	Automated Access Enforcement/Auditing				
ALL	CM-5(5)	Limit Production/Operational Privileges				
ALL	CM-6	Configuration Settings				
ALL	CM-6(1)	Automated Central Management/ Application/Verification				
ALL	CM-7	Least Functionality				
ALL	CM-7(1)	Periodic Review				
ALL	CM-7(2)	Prevent Program Execution				
ALL	CM-7(4)	Unauthorized Software/Blacklisting				
ALL	CM-8	Information System Component Inventory				
ALL	CM-8(1)	Updates During Installations/Removals				
ALL	CM-8(3)	Automated Unauthorized Component Detection				
ALL	CM-8(5)	No Duplicate Accounting of Components				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	CM-9	Configuration Management Plan				
ALL	CM-10	Software Usage Restrictions				
ALL	CM-10(1)	Open Source Software				
ALL	CM-11	User-Installed Software				
ALL	CP-1	Contingency Planning Policy and Procedures				
ALL	CP-2	Contingency Plan				
ALL	CP-2(1)	Coordinate with Related Plans				
ALL	CP-2(2)	Capacity Planning				
ALL	CP-2(3)	Resume Essential Missions/Business Functions				
ALL	CP-2(8)	Identify Critical Assets				
ALL	CP-3	Contingency Training				
ALL	CP-4	Contingency Plan Testing				
Y2	CP-4(1)	Coordinate with Related Plans				
Y2	CP-6	Alternate Storage Site				
Y2	CP-6(1)	Separation from Primary Site				
Y2	CP-6(3)	Accessibility				
Y2	CP-7	Alternate Processing Site				
Y2	CP-7(1)	Separation from Primary Site				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y2	CP-7(2)	Accessibility				
Y2	CP-7(3)	Priority of Service				
Y2	CP-8	Telecommunications Services				
Y2	CP-8(1)	Priority of Service Provisions				
Y2	CP-8(2)	Single Points of Failure				
Y2	CP-9	Information System Backup				
ALL	CP-9(1)	Testing for Reliability/Integrity				
Y2	CP-10	Information System Recovery and Reconstitution				
Y2	CP-10(2)	Transaction Recovery				
ALL	IA-1	Identification and Authentication Policy and Procedures				
ALL	IA-2	Identification and Authentication (Organizational Users)				
ALL	IA-2(1)	Network Access to Privileged Accounts				
ALL	IA-2(2)	Network Access to Non-Privileged Accounts				
ALL	IA-2(3)	Local Access to Privileged Accounts				
ALL	IA-2(8)	Network Access to Privileged Accounts - Replay Resistant				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	IA-2(11)	Remote Access – Separate Device				
Y1	IA-3	Device Identification and Authentication				
Y1	IA-4	Identifier Management				
ALL	IA-5	Authenticator Management				
Y1	IA-5(1)	Password-Based Authentication				
Y1	IA-5(2)	PKI-Based Authentication				
Y1	IA-5(3)	In-Person or Trusted Third-Party Registration				
Y1	IA-5(7)	No Embedded Unencrypted Static Authenticators				
Y1	IA-5(11)	Hardware Token-Based Authentication				
Y1	IA-6	Authenticator Feedback				
Y1	IA-7	Cryptographic Module Authentication				
Y1	IA-8	Identification and Authentication (Non-Organizational Users)				
ALL	IR-1	Incident Response Policy and Procedures				
ALL	IR-2	Incident Response Training				
ALL	IR-3	Incident Response Testing				
Y3	IR-3(2)	Coordination with Related Plans				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y3	IR-4	Incident Handling				
Y3	IR-4(1)	Automated Incident Handling Processes				
Y3	IR-5	Incident Monitoring				
Y3	IR-6	Incident Reporting				
Y3	IR-6(1)	Automated Reporting				
Y3	IR-7	Incident Response Assistance				
Y3	IR-7(1)	Automation Support for Availability of Information/Support				
ALL	IR-8	Incident Response Plan				
Y3	IR-9	Information Spillage Response				
ALL	MA-1	System Maintenance Policy and Procedures				
Y3	MA-2	Controlled Maintenance				
Y3	MA-3	Maintenance Tools				
Y3	MA-3(1)	Inspect Tools				
Y3	MA-3(2)	Inspect Media				
Y3	MA-3(3)	Prevent Unauthorized Removal				
Y3	MA-4	Non-local Maintenance				
Y3	MA-4(1)	Auditing and Review				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y3	MA-4(2)	Document Nonlocal Maintenance				
Y3	MA-4(3)	Comparable Security/Sanitization				
Y3	MA-5	Maintenance Personnel				
Y3	MA-6	Timely Maintenance				
ALL	MP-1	Media Protection Policy and Procedures				
Y3	MP-2	Media Access				
Y3	MP-3	Media Marking				
Y3	MP-4	Media Storage				
Y3	MP-5	Media Transport				
Y3	MP-5(4)	Cryptographic Protection				
Y3	MP-6	Media Sanitization				
Y3	MP-6(1)	Review/Approve/Track/Document/Verify				
ALL	MP-6(2)	Equipment Testing				
Y3	MP-7	Media Use				
Y3	MP-7(1)	Prohibit Use Without Owner				
Y3	MP-CMS-1	Media Related Records				
ALL	PE-1	Physical and Environmental Protection Policy and Procedures				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y1	PE-2	Physical Access Authorizations				
Y1	PE-2(1)	Access By Position/Role				
ALL	PE-3	Physical Access Control				
Y1	PE-4	Access Control for Transmission Medium				
Y1	PE-5	Access Control for Output Devices				
Y1	PE-6	Monitoring Physical Access				
Y1	PE-6(1)	Intrusion Alarms/Surveillance Equipment				
Y1	PE-8	Visitor Access Records				
Y1	PE-9	Power Equipment and Cabling				
Y1	PE-10	Emergency Shutoff				
Y1	PE-11	Emergency Power				
Y1	PE-12	Emergency Lighting				
Y1	PE-13	Fire Protection				
Y1	PE-13(1)	Detection Devices/Systems				
Y1	PE-13(2)	Suppression Devices/Systems				
Y1	PE-13(3)	Automatic Fire Suppression				
Y1	PE-14	Temperature and Humidity Controls				
Y1	PE-15	Water Damage Protection				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y1	PE-16	Delivery and Removal				
Y1	PE-17	Alternate Work Site				
Y1	PE-18	Location of Information System Components				
ALL	PL-1	Security Planning Policy and Procedures				
ALL	PL-2	System Security Plan (SSP)				
ALL	PL-2(3)	Plan/Coordinate with Other Organizational Entities				
ALL	PL-4	Rules of Behavior				
Y2	PL-4(1)	Social Media and Networking Restrictions				
Y2	PL-8	Information Security Architecture				
ALL	PS-1	Personnel Security Policy and Procedures				
ALL	PS-2	Position Risk Designation				
Y1	PS-3	Personnel Screening				
Y1	PS-4	Personnel Termination				
Y1	PS-5	Personnel Transfer				
ALL	PS-6	Access Agreements				
Y1	PS-7	Third-Party Personnel Security				
Y1	PS-8	Personnel Sanctions				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	RA-1	Risk Assessment Policy and Procedures				
Y2	RA-2	Security Categorization				
ALL	RA-3	Risk Assessment				
ALL	RA-5	Vulnerability Scanning				
ALL	RA-5(1)	Update Tool Capability				
ALL	RA-5(2)	Update by Frequency/Prior to New Scan/When Identified				
ALL	RA-5(3)	Breadth/Depth of Coverage				
ALL	RA-5(5)	Privileged Access				
ALL	SA-1	System and Services Acquisition Policy and Procedures				
Y3	SA-2	Allocation of Resources				
All	SA-3	System Development Life Cycle				
Y3	SA-4	Acquisition Process				
Y3	SA-4(1)	Functional Properties of Security Controls				
Y3	SA-4(2)	Design/Implementation Information for Security Controls				
Y3	SA-4(9)	Functions/Ports/Protocols/Services In Use				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y3	SA-5	Information System Documentation				
Y3	SA-8	Security Engineering				
Y3	SA-9	External Information System Services				
Y3	SA-9(1)	Risk Assessments/Organizational Approvals				
Y3	SA-9(2)	Identification of Functions/Ports/Protocols/Services				
Y3	SA-9(5)	Processing, Storage, and Service Location				
Y3	SA-10	Developer Configuration Management				
Y3	SA-11	Developer Security Testing and Evaluation				
Y3	SA-11(1)	Static Code Analysis				
Y3	SA-22	Unsupported System Components				
ALL	SC-1	System and Communications Protection Policy and Procedures				
Y1	SC-2	Application Partitioning				
Y1	SC-4	Information In Shared Resources				
ALL	SC-5	Denial of Service Protection				
Y1	SC-6	Resource Availability				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	SC-7	Boundary Protection				
ALL	SC-7(3)	Access Points				
ALL	SC-7(4)	External Telecommunications Services				
ALL	SC-7(5)	Deny by Default/Allow by Exception				
ALL	SC-7(7)	Prevent Split Tunneling for Remote Devices				
ALL	SC-7(8)	Route Traffic to Authenticated Proxy Servers				
ALL	SC-7(12)	Host-Based Protection				
ALL	SC-7(13)	Isolation of Security Tools/Mechanisms/Support Components				
ALL	SC-7(18)	Fail Secure				
ALL	SC-8	Transmission Confidentiality and Integrity				
ALL	SC-8(1)	Cryptographic or Alternate Physical Protection				
ALL	SC-8(2)	Pre/Post Transmission Handling				
Y1	SC-10	Network Disconnect				
Y1	SC-12	Cryptographic Key Establishment and Management				
Y1	SC-12(2)	Symmetric Keys				
ALL	SC-13	Cryptographic Protection				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y1	SC-15	Collaborative Computing Devices				
Y1	SC-17	Public Key Infrastructure Certificates				
Y1	SC-18	Mobile Code				
Y1	SC-19	Voice Over Internet Protocol				
Y1	SC-20	Secure Name / Address Resolution Service (Authoritative Source)				
Y1	SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)				
Y1	SC-22	Architecture and Provisioning for Name/Address Resolution Service				
Y1	SC-23	Session Authenticity				
Y1	SC-28	Protection of Information at Rest				
Y1	SC-32	Information System Partitioning				
Y1	SC-39	Process Isolation				
ALL	SC-ACA-1	Electronic Mail				
ALL	SC-ACA-2	FAX Usage				
ALL	SI-1	System and Information Integrity Policy and Procedures				
ALL	SI-2	Flaw Remediation				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	SI-2(1)	Central Management				
ALL	SI-2(2)	Automated Flaw Remediation Status				
Y2	SI-3	Malicious Code Protection				
Y2	SI-3(1)	Central Management				
Y2	SI-3(2)	Automatic Updates				
ALL	SI-4	Information System Monitoring				
ALL	SI-4(1)	System-Wide Intrusion Detection System				
ALL	SI-4(2)	Automated Tools for Real-Time Analysis				
ALL	SI-4(4)	Inbound and Outbound Communications Traffic				
ALL	SI-4(5)	System-Generated Alerts				
ALL	SI-4(14)	Wireless Intrusion Detection				
Y2	SI-5	Security Alerts, Advisories, and Directives				
Y2	SI-6	Security Function Verification				
ALL	SI-7	Software, Firmware, and Information Integrity				
ALL	SI-7(1)	Integrity Checks				
ALL	SI-7(7)	Integration of Detection and Response				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y2	SI-8	Spam Protection				
Y2	SI-8(1)	Central Management				
Y2	SI-8(2)	Automatic Updates				
ALL	SI-10	Information Input Validation				
Y2	SI-11	Error Handling				
Y2	SI-12	Information Handling and Retention				
Y2	SI-16	Memory Protection				
ALL	PM-1	Information Security Program Plan				
Y2	PM-2	Senior Information Security Officer				
Y2	PM-3	Information Security Resources				
Y2	PM-4	Plan of Action and Milestones Process				
Y2	PM-5	Information System Inventory				
Y2	PM-6	Information Security Measures of Performance				
Y2	PM-7	Enterprise Architecture				
Y2	PM-8	Critical Infrastructure Plan				
Y2	PM-9	Risk Management Strategy				
Y2	PM-10	Security Authorization Process				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
Y2	PM-11	Mission/Business Process Definition				
Y2	PM-12	Insider Threat Program				
Y2	PM-13	Information Security Workforce				
Y2	PM-14	Testing, Training, and Monitoring				
Y2	PM-15	Contacts with Security Groups and Associations				
Y2	PM-16	Threat Awareness Program				
ALL	AP-1	Authority to Collect				
ALL	AP-2	Purpose Specification				
ALL	AR-1	Governance and Privacy Program				
ALL	AR-2	Privacy Impact and Risk Assessment				
ALL	AR-3	Privacy Requirements for Contractors and Service Providers				
ALL	AR-4	Privacy Monitoring and Auditing				
ALL	AR-5	Privacy Awareness and Training				
N/A	AR-6	Privacy Reporting	Not Applicable for Non-Fed Entities			

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	AR-7	Privacy-enhanced System Design and Development				
ALL	AR-8	Accounting of Disclosures				
ALL	DI-1	Data Quality				
ALL	DI-1(1)	Validate PII				
ALL	DI-1(2)	Re-Validate PII				
N/A	DI-2	Data Integrity and Data Integrity Board	Not Applicable for Non-Fed Entities			
N/A	DI-2(1)	Publish Agreements on Website	Not Applicable for Non-Fed Entities			
ALL	DM-1	Minimization of PII				
ALL	DM-1(1)	Minimization of PII/Locate/Remove/Redact/Anonymize PII				
ALL	DM-2	Data Retention and Disposal				
ALL	DM-2(1)	Data Retention and Disposal / System Configuration				
ALL	DM-3	Minimization of use of PII Used in Testing, Training, and Research				
ALL	DM-3(1)	Minimization of PII Used in Testing, Training, and Research / Risk Minimization Techniques				
ALL	IP-1	Consent				

SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Annual Security and Privacy Attestation Report

Test Year	Control	Control Name	Test Result	Type of Test/Audit	Date Tested	POA&M Weakness Identifier
ALL	IP-1(1)	Mechanism Supporting Itemized or Tiered Consent				
ALL	IP-2	Individual Access				
ALL	IP-3	Redress				
ALL	IP-4	Complaint Management				
ALL	IP-4(1)	Complaint Management / Response Time				
ALL	SE-1	Inventory of PII				
ALL	SE-2	Privacy Incident Response				
ALL	TR-1	Privacy Notice				
ALL	TR-1(1)	Real-time or Layered Notice				
N/A	TR-2	System of Records Notices and Privacy Act Statements	Not Applicable for Non-Fed Entities			
N/A	TR-2(1)	Public Website Publication	Not Applicable for Non-Fed Entities			
ALL	TR-3	Dissemination of Privacy Program Information				
ALL	UL-1	Internal Use				
ALL	UL-2	Information Sharing with Third Parties				

Self- Attestation for Year:

(e.g., June 2015 – June 2016)

Date Completed:

System Security Officer

Signature

Date

Privacy Officer

Signature

Date

Business Owner

Signature

Date