Centers for Medicare & Medicaid Services

Affordable Care Act (ACA) Health Insurance Administering Entity

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

Final

Version 3.2

Version Date: February 24, 2022

Record of Changes

Version Number	Version Date	Author/ Owner	A=Add, M=Modify, D=Delete	Description of Change	Substantive Change [Y/N]
1.0	10/2014	-	N/A	Final draft	N/A
2.0	3/2016	-	A	Final Draft (Privacy Updates)	Y
2.1	3/2018	-	M	Final (updated for 2018)	N
2.2	3/2019	Dennis Cooper	M	Final (updated for 2019)	Y
2.3	3/2020	S. Sean Jensen	M	Final (updated for 2020)	N
3.0	3/24/2021	Chris Day	A, M	Added verbiage to align with new SAP, Workbook, and updated SAR template. Added section with instruction for Assessor Workbook. Clarified language related to AA process and requirements. Rearranged sections for better document flow. Formatting and wording changes.	Y
3.1	10/3/2021	Luis Effio, Danielle Andrews	A, M	Updated ISRA requirements in section 5. Updated Annual Attestation requirements in section 10.2. Added Controls by Attestation Year tables (Appendix A). Formatting and language changes.	Y
3.2	2/24/2022	Luis Effio	D, M	Removed some detailed references to the SAW. Removed the 'Controls by Attestation Year' tables. Corrected section references. Updated 'Purpose' section	Y

Table of Contents

1. Introduction

The *Annual Security and Privacy Attestation Procedures for the Affordable Care Act (ACA)*[1] Information Systems provides guidance for the annual attestation of the *Minimum Acceptable Risk Standards for Exchanges (MARS-E)*[2] 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.

Effective January 1, 2022:

The due date for submissions of annual attestations changes from the static date of June 30th to the AE's ATC anniversary date. Refer to Section 9.2 for additional information regarding these requirement changes.

2. Purpose

This document provides guidance and direction for:

- Ensuring ACA systems comply with MARS-E.
- Testing at least one-third (1/3) of the MARS-E security and privacy controls annually.
- Reviewing and updating ACA systems security and privacy documentation.
- Completing the Security and Privacy Controls tab of the Security and Privacy Assessment Workbook (SAW)[3].
- Submitting the Security and Privacy Assessment Plan (SAP)[4], Security and Privacy Assessment Report (SAR)[5], and SAW.
- Completing and submitting the Annual Security and Privacy Attestation Memorandum[6].

3. Requirements Background

The basis for the annual security and privacy attestation is the MARS-E 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

[1] Available at https://zone.cms.gov/document/annual-security-and-privacy-attestation-procedure-aca-systems
[2] Available at https://zone.cms.gov/document/minimum-acceptable-risk-standards-exchanges-mars-e-suite
[3] Available at https://zone.cms.gov/document/ae-security-and-privacy-assessor-workbook
[4] Available at https://zone.cms.gov/document/framework-independent-assessment-security-and-privacy-controls
[5] Id.
[6] Available at https://zone.cms.gov/document/annual-security-and-privacy-attestation-procedure-aca-systems

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 report artifacts provided to CMS helps to identify and address systemic security and privacy issues. It also provides a detailed understanding of the current security and privacy posture associated with the broader ACA program.

4. 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:
  1. Control families for current year (See the SAW for instructions).
  2. Controls to be tested annually (See the SAW for instructions).
  3. Supplemental controls to include:
     - 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 for one year.
     - Controls impacted by changes to the system environment during the current year.
     - Controls with weaknesses that were discovered during the last assessment.
     - Additional controls that need to be tested as determined by the AE or CMS.
- Complete the Information Security Risk Assessment (ISRA) as part of the AE's internal process. The ISRA is no longer a required deliverable to CMS but should be available at CMS' request. The ISRA will determine:
  1. Significant changes to business objectives or overall mission importance.
  2. Significant changes to the security state due to new or modified federal legislation, regulations, directives, policies, standards, or guidance.
  3. Effectiveness of security controls changed during the past year.
- Identify 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.
- Review and evaluate ACA security and privacy documentation by the AE. The assessment and resulting attestation documents must be submitted to CMS.
  1. 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.
  2. 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:
  1. Interconnection Security Agreement (ISA).
  2. Computer Matching Agreement (CMA).
  3. Information Exchange Agreement (IEA).
  4. Other forms of agreements such as data use agreements.

5. Annual Security and Privacy Assessment Options

The annual security and privacy control attestation may be conducted by the AE business owner, the system owner, the system developer/maintainer, or a Third-Party Independent Assessor.

There are two options for completing annual attestations:

Self-Assessment

AEs perform a self-assessment annually for 1/3 of the MARS-E security and privacy controls and submit documentation described in Section 6 of this document. At the end of Y3 of the ATC cycle, a full assessment of ALL MARS-E controls must be performed for ATC renewal. Refer to the 'Security and Privacy Controls' tab of the SAW for the full list of controls by attestation year.

Third-Party Independent Assessment

AEs perform a third-party independent assessment annually for 1/3 of the MARS-E security and privacy controls and submits documentation described in Section 7 of this document. At the end of Y3 ATC cycle, the third-party independent assessment performed for Y1, Y2, and Y3 are combined to be used for the renewal of an ATC. Refer to the 'Security and Privacy Controls' tab of the SAW for the full list of controls by attestation year.

6. Annual Security and Privacy Self-Assessment

6.1 Self-Assessment Package

When a self-assessment is performed for the annual attestation, the test results, including the required penetration testing, must be documented and submitted to CMS utilizing the following documents:

- SAW

- Annual Attestation Memorandum

All findings identified during a self-assessment need to be captured in the POA&M and clearly mapped to the SAW.

6.1.1 Self-Assessment Options

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

- Continuous monitoring activities
- Ongoing testing and evaluation of security and privacy associated with the system development life cycle
- Internal privacy risk assessments
- Various internal security and privacy audits
- 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 and privacy controls are reviewed and validated against the required MARS-E security and privacy controls. For testing the controls, the procedures for each control are documented in the MARS-E Document Suite[7].

Contact your assigned CMS Information System Security Officer (ISSO) for inquiries about using alternative testing methods.

6.2 Security and Privacy Assessor Workbook Instructions for a Self-Assessment

Refer to the SAW for detailed instructions on completing the 'Security and Privacy Controls' tab and all other required tabs.

Section 6.2.1 also provides the steps to select 1/3 of the MARS-E security and privacy controls for a self-assessment using the SAW.

NOTE: At least one of the assessment method columns in the 'Security and Privacy Controls' tab of the SAW (Examine, Interview, and Test), must be completed for the required security and privacy controls outlined in the MARS-E Document Suite[8]. Add comments in the 'Comments' column, if necessary.

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

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

6.2.1 Security and Privacy Controls Tab Instructions

In the 'Attestation Year' column (D), identify the attestation being conducted by clicking the **filter** drop down icon in **Row 11-Column D**. In the drop-down list, there is a clickable box to the left of every selection. Choose the correct annual attestation year, from the following options:

Annual Attestation Year 1

For an annual attestation being conducted for **Year 1** security and privacy controls, choose the type of annual self-assessment that applies.

- **For a self-assessment with NO supplemental controls**

  1. Uncheck **"Select All"**.
  2. Check the **"Y1"** box. All **Y1** security and privacy controls will be displayed.
  3. For each control selected, populate the cells for AT LEAST ONE of the assessment methods (Examine, Interview, and Test).
  4. Add comments in the 'Comments' column, if necessary.

- **For a self-assessment with supplemental controls**

  1. Uncheck **"Select All"**.
  2. Check **"Blanks"**.
  3. After checking **"Blanks"** in the drop-down list, scroll down to the security and/or privacy control(s) that need to be added to this year's annual attestation.
  4. In the cell of column D for each specific supplemental control, click the drop-down icon and select **"Supplemental"**.
  5. Scroll up to the top of the 'Security and Privacy Controls' tab, click the **filter** drop-down icon in **Row 11-Column D** again.
  6. Check the **"Supplemental"** and **"Y1"** boxes.
  7. Uncheck **"Blanks"**. All **Y1** and **supplemental** security and/or privacy controls to be assessed will be displayed.
  5. For each control selected, populate the cells for AT LEAST ONE of the assessment methods (Examine, Interview, and Test).
  6. Add comments in the 'Comments' column, if necessary.

Annual Attestation Year 2

For an annual attestation being conducted for **Year 2** security and privacy controls, choose the type of annual self-assessment that applies.

- **For a self-assessment with NO supplemental controls**

  1. Uncheck **"Select All"**.
  2. Check the **"Y2"** box. All **Y2** security and/or privacy controls will be displayed.
  3. For each control selected, populate the cells for AT LEAST ONE of the assessment methods (Examine, Interview, and Test).
  4. Add comments in the 'Comments' column, if necessary.

- **For a self-assessment with supplemental controls**

  1. Uncheck **"Select All"**.
  2. Check **"Blanks"**.

3. After checking **"Blanks"** in the drop-down list, scroll down to the security and/or privacy control(s) that need to be added to this year's annual attestation.
4. In the cell of column D for each specific supplemental control, click the drop-down icon and select **"Supplemental"**.
5. Scroll up to the top of the 'Security and Privacy Controls' tab, click the **filter** drop-down icon in **Row 11-Column D** again.
6. Check the **"Supplemental"** and **"Y2"** boxes.
7. Uncheck **"Blanks"**. All **Y2** and **supplemental** security and/or privacy controls to be assessed will be displayed.
8. For each control selected, populate the cells for AT LEAST ONE of the assessment methods (Examine, Interview, and Test).
9. Add comments in the 'Comments' column, if necessary.

Annual Attestation Year 3

For an annual attestation being conducted for **Year 3** security and privacy controls, choose the type of annual self-assessment that applies.

- **For a self-assessment with NO supplemental controls**

1. Uncheck **"Select All"**.
2. Check the **"Y3"** box. All **Y3** security and/or privacy controls will be displayed.
3. For each control selected, populate the cells for AT LEAST ONE of the assessment methods (Examine, Interview, and Test).
4. Add comments in the 'Comments' column, if necessary.

- **For a self-assessment with supplemental controls**

1. Uncheck **"Select All"**.
2. Check **"Blanks"**.
3. After checking **"Blanks"** in the drop-down list, scroll down to the security and/or privacy control(s) that need to be added to this year's annual attestation.
4. In the cell of column D for each specific supplemental control, click the drop-down icon and select **"Supplemental"**.
5. Scroll up to the top of the 'Security and Privacy Controls' tab, click the **filter** drop-down icon in **Row 11-Column D** again.
6. Check the **"Supplemental"** and **"Y3"** boxes.
7. Uncheck **"Blanks"**. All **Y3** and **supplemental** security and/or privacy controls to be assessed will be displayed.
8. For each control selected, populate the cells for AT LEAST ONE of the assessment methods (Examine, Interview, and Test).
9. Add comments in the 'Comments' column, if necessary.

NOTE: If a full third-party independent assessment is being leveraged in **Y3**, follow the instructions for conducting this type of assessment in the *Framework for the Independent Assessment of Security and Privacy Controls*[9].

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

7. Annual Security and Privacy Third-Party Independent Assessment

7.1 Third-Party Independent Assessment Package

Refer to the *Framework for the Independent Assessment of Security and Privacy Controls*[10] for information on how to conduct a third-party independent assessment. When a third-party independent assessment is performed for an annual attestation, the test plan and the results, including the required penetration testing, must be documented and submitted to CMS utilizing the following documents:

- Security and Privacy Assessment Plan (SAP)
- Security and Privacy Assessment Report (SAR)
- Security and Privacy Assessor Workbook (SAW)
- Security and Privacy Attestation Memorandum

A separate SAR, SAW, and Annual Attestation Memorandum will be required for Y1, Y2, and Y3 security and privacy control testing and utilized in combination for the renewal of an ATC.

All findings identified during a third-party independent assessment need to be captured in the POA&M and clearly mapped to the SAR and SAW.

7.1.1 Third-Party Independent Assessment Options

As an option, the AE may fulfill the third-party independent assessment requirement by utilizing the results from an alternate Independent Assessment. The alternate third-party independent assessment must have the following criteria below to be considered:

- True independence was determined.
- The third-party independent assessment was performed within the boundary of the ACA system.
- The applicable MARS-E security and privacy controls were tested.

Depending on the extent of testing from other sources, the organization may need to perform additional testing to ensure all security and privacy controls are reviewed and validated against the required MARS-E security and privacy controls. For testing the controls, the procedures for each control are documented in the MARS-E Document Suite[11].

The use of an alternate third-party independent assessment must be approved by CMS prior to submission of the security assessment package.

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

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

7.2 Security and Privacy Assessor Workbook Instructions for a Third-Party Independent Assessment

Refer to the SAW for detailed instructions on completing the 'Security and Privacy Controls' tab and all other required tabs.

Section 7.2.1 also provides the steps to select 1/3 of the MARS-E security and privacy controls for a third-party independent assessment using the SAW.

NOTE: ALL of the assessment method columns in the 'Security and Privacy Control' tab of the SAW (Examine, Interview, and Test), must be completed for the required security and privacy controls outlined in the MARS-E Document Suite[12]. Add comments in the 'Comments' column, if necessary.

7.2.1 Security and Privacy Controls Tab Instructions

In the 'Attestation Year' column (D), identify the Attestation being conducted by clicking the **Filter** drop down icon in **Row 11-Column D**. In the drop-down list, there is a clickable box to the left of every selection. Choose the correct annual attestation year, from the following options:

Annual Attestation Year 1

For an annual attestation being conducted for **Year 1** security and privacy controls, choose the type of annual third-party independent assessment that applies.

- **For a third-party independent assessment with NO supplemental controls**

  1. Uncheck **"Select All"**.
  2. Check the **"Y1"** box. All **Y1** security and/or privacy controls will be displayed.
  3. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).
  4. Add comments in the 'Comments' column, if necessary.

- **For a third-party independent assessment with NO supplemental controls**

  1. Uncheck **"Select All"**.
  2. Check **"Blanks"**.
  3. After checking **"Blanks"** in the drop-down list, scroll down to the security and/or privacy control(s) that need to be added to this year's annual attestation.
  4. In the cell of column D for each specific supplemental control, click the drop-down icon and select **"Supplemental"**.
  5. Scroll up to the top of the 'Security and Privacy Controls' tab, click the **filter** drop-down icon in **Row 11-Column D** again.
  6. Check the **"Supplemental"** and **"Y1"** boxes.
  7. Uncheck **"Blanks"**. All **Y1** and **supplemental** security and/or privacy controls to be assessed will be displayed.
  8. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).

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

9. Add comments in the 'Comments' column, if necessary.

Annual Attestation Year 2

For an annual attestation being conducted for **Year 2** security and privacy controls, choose the type of annual third-party independent assessment that applies.

- **For a third-party independent assessment with NO supplemental controls**

1. Uncheck **"Select All"**.
2. Check the **"Y2"** box. All **Y2** security and/or privacy controls will be displayed.
3. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).
4. Add comments in the 'Comments' column, if necessary.

- **For a third-party independent assessment with NO supplemental controls**

1. Uncheck **"Select All"**.
2. Check **"Blanks"**.
3. After checking **"Blanks"** in the drop-down list, scroll down to the security and/or privacy control(s) that need to be added to this year's annual attestation.
4. In the cell of column D for each specific supplemental control, click the drop-down icon and select **"Supplemental"**.
5. Scroll up to the top of the 'Security and Privacy Controls' tab, click the **filter** drop-down icon in **Row 11-Column D** again.
6. Check the **"Supplemental"** and **"Y2"** boxes.
7. Uncheck **"Blanks"**. All **Y2** and **supplemental** security and/or privacy controls to be assessed will be displayed.
8. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).
9. Add comments in the 'Comments' column, if necessary.

Annual Attestation Year 3

For an annual attestation being conducted for **Year 3** security and privacy controls, choose the type of annual third-party independent assessment that applies.

- **For a third-party independent assessment with NO supplemental controls**

1. Uncheck **"Select All"**.
2. Check the **"Y3"** box. All **Y3** security and/or privacy controls will be displayed.
3. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).
4. Add comments in the 'Comments' column, if necessary.

- **For a third-party independent assessment with NO supplemental controls**

1. Uncheck **"Select All"**.
2. Check **"Blanks"**.
3. After checking **"Blanks"** in the drop-down list, scroll down to the security and/or privacy control(s) that need to be added to this year's annual attestation.
4. In the cell of column D for each specific supplemental control, click the drop-down icon and select **"Supplemental"**.

5. Scroll up to the top of the 'Security and Privacy Controls' tab, click the **filter** drop-down icon in **Row 11-Column D** again.
6. Check the **"Supplemental"** and **"Y3"** boxes.
7. Uncheck **"Blanks"**. All **Y3** and **supplemental** security and/or privacy controls to be assessed will be displayed.
8. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).
9. Add comments in the 'Comments' column, if necessary.

- **For a third-party independent assessment with NO supplemental controls**

1. Uncheck **"Select All"**.
2. Check the box next to **"All Controls"**. All security and privacy controls from the approved MARS-E SSP will be displayed.
3. For each control selected, populate the cells for ALL of the assessment methods (Examine, Interview, and Test).
4. Add comments in the 'Comments' column, if necessary.

8. Security and Privacy Annual Attestation Memorandum

The Security and Privacy Annual Attestation Memorandum must be used to complete a self-assessment or third-party independent assessment. The signatories on the memorandum 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 memorandum requires the latest review date for the following security documents:

- Authority to Connect (ATC)
- Organization Continuous Monitoring Policies and Procedures
- Risk Assessments
- System Security Plan (SSP) and supporting Attachments including Security and Privacy Control Implementations
- Security and Privacy Assessment Report (SAR)
- Security and Privacy Assessment Workbook (SAW)
- Contingency Plan (CP)
- Contingency Plan (CP) Test
- Privacy Impact Assessment (PIA)
- Plan of Actions & Milestones (POA&M)
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- Computer Matching Agreement (CMA)

- Information Exchange Agreement (IEA)
- Interconnection Security Agreement (ISA)

With the exception of the SAW and Annual Attestation Memorandum for a self-assessment and the SAR, SAW, and Annual Attestation Memorandum for a third-party independent assessment, the aforementioned documents are not required to be submitted to CMS as part of the annual attestation submission, but need to be available should CMS request them.

9. Submission Timeframe

9.1 Submission Prior to Annual Attestation Kick-Off

For a self-assessment, a SAP submission will not be required.

For a third-party independent assessment, the SAP is due 30 days prior to the start of the assessment.

9.2 Submissions Upon Completion of an Annual Attestation

For a self-assessment, the Security and Privacy Assessor Workbook and Annual Attestation Memorandum must be submitted to CMS annually on the ATC anniversary date or the first business day after, should the ATC anniversary date fall on a weekend.

For a third-party independent assessment, the SAR, SAW, and Annual Attestation Memorandum must be submitted to CMS:

- Y1 and Y2: Annually on the ATC anniversary date or the first business day after, should the ATC anniversary date fall on a weekend.
- Y3: 90 days prior to the ATC anniversary date or the first business day after, should the ATC anniversary date fall on a weekend.

Any expected delays of attestation submissions must be communicated to the assigned CMS ISSO. AEs must receive prior approval from the CMS ISSO for attestation submissions that will occur after the due date to ensure accurate compliance tracking.

Appendix A. Acronym List

ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
AR	MARS-E Privacy Impact and Risk Assessment Control
ATC	Authority to Connect
CA	Security Assessment and Authorization
CIDR	Classless Inter-Domain Routing
CMA	Legal Agreements such as the Computer Matching Agreement
CMP	Configuration Management Plan
CMS	Centers for Medicare & Medicaid Services
CP	Contingency Planning
CPT	Contingency Plan Test
FISMA	Federal Information Security Management Act
GAO	General Accounting Office
HHS	Department of Health and Human Services
HTTPS	Hypertext Transfer Protocol Secure
IEA	Information Exchange Agreement
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISRA	Information Security Risk Assessment
ISSO	Information System Security Officer
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MTD	Maximum Tolerable Disruption
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action & Milestones
RA	Risk Assessment, a Security Control family
RPO	Recovery Point Objective

RTO	Recovery Time Objective
SAP	Security and Privacy Assessment Plan
SAR	Security and Privacy Assessment Report
SAW	Security and Privacy Assessment Workbook
SSP	System Security and Privacy Plan
Y1	Attestation Year 1
Y2	Attestation Year 2
Y3	Attestation Year 3